Cisco IOS Security Command Reference

April 2011

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Cisco IOS Security Command Reference

CONTENTS

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

The *Cisco IOS Security Command Reference* contains commands that are used to configure Cisco IOS security features for your Cisco networking devices; specifically, it contains commands used to perform the following functions:

- Configure authentication, authorization, and accounting (AAA).
- Configure security server protocols such as RADIUS, TACACS+, and Kerberos.

Note TACACS and Extended TACACS commands are included in Cisco IOS Release 12.2 software for backward compatibility with earlier Cisco IOS releases; however, these commands are no longer supported and are not documented for this release.

Cisco recommends using only the TACACS+ security protocol with Release 12.1 and later of Cisco IOS software.

Table 1 identifies Cisco IOS software commands available to the different versions of TACACS. Although TACACS+ is enabled through AAA and uses commands specific to AAA, there are some commands that are common to TACACS, Extended TACACS, and TACACS+. TACACS and Extended TACACS commands that are not common to TACACS+ are not documented in this release.

Table 1 TACACS Command Comparison

Cisco IOS Command	TACACS	Extended TACACS	TACACS+
aaa accounting	—	—	**yes**
aaa authentication arap	—	—	**yes**
aaa authentication enable default	—	—	**yes**
aaa authentication login	—	—	**yes**
aaa authentication ppp	—	—	**yes**
aaa authorization	—	—	**yes**
aaa group server tacacs+	—	—	**yes**
aaa new-model	—	—	**yes**
arap authentication	—	—	**yes**
arap use-tacacs	**yes**	**yes**	—
enable last-resort	**yes**	**yes**	—

Table 1 TACACS Command Comparison (continued)

Cisco IOS Command	TACACS	Extended TACACS	TACACS+
enable use-tacacs	**yes**	**yes**	—
ip tacacs source-interface	**yes**	**yes**	**yes**
login authentication	—	—	**yes**
login tacacs	**yes**	**yes**	—
ppp authentication	**yes**	**yes**	**yes**
ppp use-tacacs	**yes**	**yes**	no
server	—	—	**yes**
tacacs-server administration	**—**	—	**yes**
tacacs-server directed-request	**yes**	**yes**	**yes**
tacacs-server dns-alias-lookup	**—**	**—**	yes
tacacs-server host	**yes**	**yes**	**yes**
tacacs-server key	—	—	**yes**
tacacs-server packet	**—**	**—**	yes
tacacs-server timeout	**yes**	**yes**	yes

- Configure the following traffic filtering and firewall features:
  - Context-Based Access Control (CBAC)
  - Intrusion Detection System (IDS)
  - Port to application mapping (PAM)
  - Reflexive access lists
  - TCP Intercept
- Configure IP Security (IPSec) and encryption features such as public key infrastructure (PKI) and Internet Key Exchange (IKE).
- Configure additional security features such as passwords and privileges, IP Security Options (IPSO), Unicast Reverse Path Forwarding (uRPF), secure shell (SSH), and AutoSecure.

For information on how to configure Cisco IOS security features and configuration examples using the commands in this book, refer to the *Cisco IOS Security Configuration Guide*.

Security Commands

aaa accounting

To enable authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use RADIUS or TACACS+, use the **aaa accounting** command in global configuration mode or template configuration mode. To disable AAA accounting, use the **no** form of this command.

aaa accounting {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands** *level* | **dot1x**} {**default** | *list-name* | **guarantee-first**} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] {**radius** | **group** *group-name*}

no aaa accounting {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands** *level* | **dot1x**} {**default** | *list-name* | **guarantee-first**} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] {**radius** | **group** *group-name*}

Template Configuration Mode

aaa accounting {**delay-start** | **send stop-record authentication**} {**failure** | **success** **remote-server**}

no aaa accounting {**delay-start** | **send stop-record authentication**} {**failure** | **success** **remote-server**}

Syntax Description

auth-proxy	Provides information about all authenticated-proxy user events.
system	Performs accounting for all system-level events not associated with users, such as reloads. **Note** When system accounting is used and the accounting server is unreachable at system startup time, the system will not be accessible for approximately two minutes.
network	Runs accounting for all network-related service requests, including Serial Line Internet Protocol (SLIP), PPP, PPP Network Control Protocols (NCPs), and AppleTalk Remote Access Protocol (ARAP).
exec	Runs accounting for the EXEC shell session.
connection	Provides information about all outbound connections made from the network access server, such as Telnet, local-area transport (LAT), TN3270, packet assembler and disassembler (PAD), and rlogin.
commands *level*	Runs accounting for all commands at the specified privilege level. Valid privilege level entries are integers from 0 through 15.
dot1x	Provides information about all IEEE 802.1x-related user events.
default	Uses the listed accounting methods that follow this keyword as the default list of methods for accounting services.

list-name	Character string used to name the list of at least one of the following accounting methods: • **group radius**—Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command. • **group tacacs+**—Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command. • **group** *group-name*—Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group *group-name* argument.
guarantee-first	Guarantees system accounting as the first record.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration. • VRF is used *only* with system accounting.
start-stop	Sends a “start” accounting notice at the beginning of a process and a “stop” accounting notice at the end of a process. The “start” accounting record is sent in the background. The requested user process begins regardless of whether the “start” accounting notice was received by the accounting server.
stop-only	Sends a “stop” accounting record for all cases including authentication failures regardless of whether the **aaa accounting send stop-record authentication failure** command is configured.
none	Disables accounting services on this line or interface.
broadcast	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.
radius	Runs the accounting service for RADIUS.

group *group-name*	Specifies the accounting method list. Enter at least one of the following keywords: • **auth-proxy**—Creates a method list to provide accounting information about all authenticated hosts that use the authentication proxy service. • **commands**—Creates a method list to provide accounting information about specific, individual EXEC commands associated with a specific privilege level. • **connection**—Creates a method list to provide accounting information about all outbound connections made from the network access server. • **exec**—Creates a method list to provide accounting records about user EXEC terminal sessions on the network access server, including username, date, and start and stop times. • **network**—Creates a method list to provide accounting information for SLIP, PPP, NCPs, and ARAP sessions. • **resource**—Creates a method list to provide accounting records for calls that have passed user authentication or calls that failed to be authenticated. • **tunnel**—Creates a method list to provide accounting records (Tunnel-Start, Tunnel-Stop, and Tunnel-Reject) for virtual private dialup network (VPDN) tunnel status changes. • **tunnel-link**—Creates a method list to provide accounting records (Tunnel-Link-Start, Tunnel-Link-Stop, and Tunnel-Link-Reject) for VPDN tunnel-link status changes.
delay-start	Delays PPP network start records until peer IP address is known.
send	Sends records to the accounting server.
stop-record	Generates stop records for a specified event.
authentication	Generates stop records for authentication.
failure	Generates stop records for authentication failures.
success	Generates stop records for authenticated users.
remote-server	Specifies that the users are successfully authenticated through access-accept, by a remote AAA server.

Defaults

AAA accounting is disabled.

Command Modes

Global configuration (config)
Template configuration (config-template)

Command History

Release	Modification
12.0(5)T	This command was modified. The Group server support was added.
12.1(1)T	This command was modified. The **broadcast** keyword was added on the Cisco AS5300 and Cisco AS5800 universal access servers.
12.1(5)T	This command was modified. The **auth-proxy** keyword was added.

Release	Modification
12.2(1)DX	This command was modified. The **vrf** keyword and *vrf-name* argument were added on the Cisco 7200 series and Cisco 7401ASR series routers.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was modified. The **vrf** keyword and *vrf-name* argument were integrated into Cisco IOS Release 12.2(13)T.
12.2(15)B	This command was modified. The tunnel and tunnel-link accounting methods were introduced.
12.3(4)T	This command was modified. The tunnel and tunnel-link accounting methods were integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The **dot1x** keyword was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6. The **radius** keyword was added.

Usage Guidelines

General Information

Use the **aaa accounting** command to enable accounting and to create named method lists that define specific accounting methods on a per-line or per-interface basis. You must enable AAA services using the **aaa new-model** global configuration command.

Table 1 contains descriptions of keywords for AAA accounting methods.

Table 1 aaa accounting Methods

Keyword	Description
group radius	Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command.
group tacacs+	Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group *group-name* argument.

In Table 1, the **group radius** and **group tacacs+** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Cisco IOS software supports the following two methods of accounting:

- RADIUS—The network access server reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.

- TACACS+—The network access server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting AV pairs and is stored on the security server.

Method lists for accounting define the way accounting will be performed. Named accounting method lists enable you to designate a particular security protocol to be used on specific lines or interfaces for particular types of accounting services. Create a list by entering values for the *list-name* argument where *list-name* is any character string used to name this list (excluding the names of methods, such as RADIUS or TACACS+) and method list keywords to identify the methods to be tried in sequence as given.

If the **aaa accounting** command for a particular accounting type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines (where this accounting type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no accounting takes place.

Note System accounting does not use named accounting lists; you can define the default list only for system accounting.

For minimal accounting, include the **stop-only** keyword to send a "stop" accounting record for all cases including authentication failures. For more accounting, you can include the **start-stop** keyword, so that RADIUS or TACACS+ sends a "start" accounting notice at the beginning of the requested process and a "stop" accounting notice at the end of the process. Accounting is stored only on the RADIUS or TACACS+ server. The **none** keyword disables accounting services for the specified line or interface.

To specify an accounting configuration for a particular VRF, specify a default system accounting method list, and use the **vrf** keyword and *vrf-name* argument. System accounting does not have knowledge of VRF unless specified.

When AAA accounting is activated, the network access server monitors either RADIUS accounting attributes or TACACS+ AV pairs pertinent to the connection, depending on the security method you have implemented. The network access server reports these attributes as accounting records, which are then stored in an accounting log on the security server. For a list of supported RADIUS accounting attributes, see the appendix "RADIUS Attributes" in the*Cisco IOS Security Configuration Guide*. For a list of supported TACACS+ accounting AV pairs, see the appendix "TACACS+ Attribute-Value Pairs" in the *Cisco IOS Security Configuration Guide*.

Note The **aaa accounting** command cannot be used with TACACS or extended TACACS.

Cisco Service Selection Gateway Broadcast Accounting

To configure Cisco Service Selection Gateway (SSG) broadcast accounting, use ssg_broadcast_accounting for the *list-name* argument. For more information about configuring SSG, see the chapter "Configuring Accounting for SSG" in the *Cisco IOS Service Selection Gateway Configuration Guide*, Release 12.4.

Layer 2 LAN Switch Port

You must configure the RADIUS server to perform accounting tasks, such as logging start, stop, and interim-update messages and time stamps. To turn on these functions, enable logging of "Update/Watchdog packets from this AAA client" in your RADIUS server Network Configuration tab. Next, enable "CVS RADIUS Accounting" in your RADIUS server System Configuration tab.

You must enable AAA before you can enter the **aaa accounting** command. To enable AAA and 802.1X (port-based authentication), use the following global configuration mode commands:

- **aaa new-model**
- **aaa authentication dot1x default group radius**
- **dot1x system-auth-control**

Use the **show radius statistics** command to display the number of RADIUS messages that do not receive the accounting response message.

Use the **aaa accounting system default start-stop group radius** command to send "start" and "stop" accounting records after the router reboots. The "start" record is generated while the router is booted and the stop record is generated while the router is reloaded.

The router generates a "start" record to reach the AAA server. If the AAA server is not reachable, the router retries sending the packet four times. The retry mechanism is based on the exponential backoff algorithm. If there is no response from the AAA server, the request will be dropped.

Establishing a Session with a Router if the AAA Server is Unreachable

The **aaa accounting system guarantee-first** command guarantees system accounting as the first record, which is the default condition. In some situations, users may be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than three minutes.

To establish a console or telnet session with the router if the AAA server is unreachable when the router reloads, use the **no aaa accounting system guarantee-first** command.

Note Entering the **no aaa accounting system guarantee-first** command is not the only condition by which the console or telnet session can be started. For example, if the privileged EXEC session is being authenticated by TACACS and the TACACS server is not reachable, then the session cannot start.

Examples

The following example shows how to define a default command accounting method list, where accounting services are provided by a TACACS+ security server, set for privilege level 15 commands with a stop-only restriction.

```
aaa accounting commands 15 default stop-only group tacacs+
```

The following example shows how to defines a default auth-proxy accounting method list, where accounting services are provided by a TACACS+ security server with a start-stop restriction. The **aaa accounting** command activates authentication proxy accounting.

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization auth-proxy default group tacacs+
aaa accounting auth-proxy default start-stop group tacacs+
```

The following example shows how to define a default system accounting method list, where accounting services are provided by RADIUS security server "server1" with a start-stop restriction. The **aaa accounting** command specifies accounting for VRF "vrf1."

```
aaa accounting system default vrf vrf1 start-stop group server1
```

The following example shows how to define a default IEEE 802.1x accounting method list, where accounting services are provided by a RADIUS server. The **aaa accounting** command activates IEEE 802.1x accounting.

```
aaa new model
aaa authentication dot1x default group radius
aaa authorization dot1x default group radius
aaa accounting dot1x default start-stop group radius
```

The following example shows how to enable network accounting and send tunnel and tunnel-link accounting records to the RADIUS server. (Tunnel-Reject and Tunnel-Link-Reject accounting records are automatically sent if either start or stop records are configured.)

```
aaa accounting network tunnel start-stop group radius
aaa accounting network session start-stop group radius
```

The following example shows how to delay PPP Network start record until peer IP address is known:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# template name
Router(config-template)# aaa accounting delay-start
```

Related Commands

Command	Description
aaa authentication dot1x	Specifies one or more AAA methods for use on interfaces running IEEE 802.1X.
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
aaa group server tacacs+	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
auto command	Configures the system to automatically execute a specific EXEC command when it connects to a port.
dot1x system-auth-control	Enables port-based authentication.
radius-server host	Specifies a RADIUS server host.
show radius statistics	Displays the RADIUS statistics for accounting and authentication packets.
tacacs-server host	Specifies a TACACS+ server host.

aaa accounting (IKEv2 profile)

To enable AAA accounting for IPsec sessions, use the **aaa accounting** command in IKEv2 profile configuration mode. To disable AAA accounting, use the **no** form of this command.

aaa accounting [**psk** | **cert** | **eap**] *list-name*

no aaa accounting [**psk** | **cert** | **eap**] *list-name*

Syntax Description

psk	(Optional) Specifies a method list if the authentication method preshared key.
cert	(Optional) Specifies a method list if the authentication method is certificate based.
eap	(Optional) Specifies a method list if the authentication method is Extensible Authentication Protocol (EAP).
list-name	Name of the AAA list.

Command Default

AAA accounting is disabled.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use the **aaa accounting** command to enable and specify the method list for AAA accounting for IPsec sessions. The **aaa accounting** command can be specific to an authentication method or common to all authentication methods, but not both at the same time. If no method list is specified, the list is common across authentication methods.

Examples

The following example defines an AAA accounting configuration common to all authentication methods:

```
Router(config-ikev2-profile)# aaa accounting common-list1
```

The following example configures an AAA accounting for each authentication method:

```
Router(config-ikev2-profile)# aaa accounting psk psk-list1
Router(config-ikev2-profile)# aaa accounting cert cert-list1
Router(config-ikev2-profile)# aaa accounting eap eap-list1
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.

aaa accounting connection h323

To define the accounting method list H.323 using RADIUS as a method with either **stop-only** or **start-stop** accounting options, use the **aaa accounting connection h323** command in global configuration mode. To disable the use of this accounting method list, use the **no** form of this command.

aaa accounting connection h323 {**stop-only** | **start-stop** | **none**} [**broadcast**] **group** *groupname*

no aaa accounting connection h323 {**stop-only** | **start-stop** | **none**} [**broadcast**] **group** *groupname*

Syntax Description

stop-only	Sends a "stop" accounting notice at the end of the requested user process.
start-stop	Sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. The "start" accounting record is sent in the background. The requested user process begins regardless of whether the "start" accounting notice was received by the accounting server.
none	Disables accounting services on this line or interface.
broadcast	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.
group *groupname*	Specifies the server group to be used for accounting services. The following are valid server group names: • *string*: Character string used to name a server group. • **radius**: Uses list of all RADIUS hosts. • **tacacs+**: Uses list of all TACACS+ hosts.

Defaults

No accounting method list is defined.

Command Modes

Global configuration

Command History

Release	Modification
11.3(6)NA2	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command creates a method list called h323 and is applied by default to all voice interfaces if the **gw-accounting h323** command is also activated.

Examples

The following example enables authentication, authorization, and accounting (AAA) services, gateway accounting services, and defines a connection accounting method list (h323). The h323 accounting method lists specifies that RADIUS is the security protocol that will provide the accounting services, and that the RADIUS service will track start-stop records.

```
aaa new model
gw-accounting h323
aaa accounting connection h323 start-stop group radius
```

Related Commands

Command	Description
gw-accounting	Enables the accounting method for collecting call detail records.

aaa accounting delay-start

To delay generation of accounting "start" records until the user IP address is established, use the **aaa accounting delay-start** command in global configuration mode. To disable this functionality, use the **no** form of this command.

aaa accounting delay-start [**all**] [**vrf** *vrf-name*]

no aaa accounting delay-start [**all**] [**vrf** *vrf-name*]

Syntax Description

all	(Optional) Extends the delay of accounting "start" records to all Virtual Route Forwarding (VRF) and non-VRF users.
vrf *vrf-name*	(Optional) Extends the delay of accounting "start" records to individual VRF users.

Defaults

Accounting records are not delayed.

Command Modes

Global configuration

Command History

Release	Modification
12.1	This command was introduced.
12.2(1)DX	The **vrf** keyword and *vrf-name* argument were introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were integrated into Cisco IOS Release 12.2(13)T.
12.3(1)	The **all** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **aaa accounting delay-start** command to delay generation of accounting "start" records until the IP address of the user has been established. Use the **vrf** *vrf-name* keyword and argument to delay accounting "start" records for individual Virtual Private Network (VPN) routing and forwarding (VRF) users or use the **all** keyword for all VRF and non-VRF users.

Note The **aaa accounting delay-start** command applies only to non-VRF users. If you have a mix of VRF and non-VRF users, configure either **aaa accounting delay-start** (for non-VRF users) or **aaa accounting delay-start vrf** {*vrf-name*} (for VRF users) or **aaa accounting delay-start all** (for all VRF and non-VRF users).

Examples

The following example shows how to delay accounting "start" records until the IP address of the user is established:

```
aaa new-model
aaa authentication ppp default radius
aaa accounting network default start-stop group radius
aaa accounting delay-start
radius-server host 172.16.0.0 non-standard
radius-server key rad123
```

The following example shows that accounting "start" records are to be delayed to all VRF and non-VRF users:

```
aaa new-model
aaa authentication ppp default radius
aaa accounting network default start-stop group radius
aaa accounting delay-start all
radius-server host 172.16.0.0 non-standard
radius-server key rad123
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.
tacacs-server host	Specifies a TACACS+ server host.

aaa accounting gigawords

To enable authentication, authorization, and accounting (AAA) 64-bit, high-capacity counters, use the **aaa accounting gigawords** command in global configuration mode. To disable the counters, use the **no** form of this command. (Note that gigaword support is automatically configured unless you unconfigure it using the **no** form of the command.)

aaa accounting gigawords

no aaa accounting gigawords

Syntax Description

This command has no arguments or keywords.

Defaults

If this command is not configured, the 64-bit, high-capacity counters that support RADIUS attributes 52 and 53 are automatically enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13.7)T	This command was introduced.

Usage Guidelines

The AAA high-capacity counter process takes approximately 8 percent CPU memory for 24,000 (24 K) sessions running under steady state.

If you have entered the **no** form of this command to turn off the 64-bit counters and you want to reenable them, you will need to enter the **aaa accounting gigawords** command. Also, once you have entered the **no** form of the command, it takes a reload of the router to actually disable the use of the 64-bit counters.

Note The **aaa accounting gigawords** command does not show up in the running configuration unless the **no** form of the command is used in the configuration.

Examples

The following example shows that the AAA 64-bit counters have been disabled:

```
no aaa accounting gigawords
```

aaa accounting include auth-profile

To include authorization profile attributes for the AAA accounting records, use the **aaa accounting include auth-profile** command in global configuration mode. To disable the authorization profile, use the **no** form of this command.

aaa accounting include auth-profile {**delegated-ipv6-prefix** | **framed-ip-address** | **framed-ipv6-prefix**}

no aaa accounting include auth-profile {**delegated-ipv6-prefix** | **framed-ip-address** | **framed-ipv6-prefix**}

Syntax Description

delegated-ipv6-prefix	Includes the delegated-IPv6-Prefix profile in accounting records.
framed-ip-address	Includes the Framed-IP-Address profile in accounting records.
framed-ipv6-prefix	Includes the Framed-IPv6-Prefix profile in accounting records.

Command Default

authorization profile is included in the aaa accounting records.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced in a release earlier than Cisco IOS Release 15.1(1)T.

Usage Guidelines

The **aaa accounting include auth-profile** command can also be used for a dual-stack session if the negotiation between IPv4 and IPv6 is successful.

Examples

The following example shows how to include the delegated-IPv6-Prefix profile in the AAA accounting records:

```
Router(config)# aaa accounting include auth-profile delegated-ipv6-prefix
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.

aaa accounting-list

To enable authentication, authorization, and accounting (AAA) accounting when you are using RADIUS for Secure Socket Layer Virtual Private Network (SSL VPN) sessions, use the **aaa accounting-list** command in global configuration mode. To disable the AAA accounting, use the **no** form of this command.

aaa accounting-list *aaa-list*

no aaa accounting-list *aaa-list*

Syntax Description

aaa-list	Name of the AAA accounting list that has been configured under global configuration.

Defaults

AAA accounting is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Before configuring this command, ensure that the AAA accounting list has already been configured under global configuration.

Examples

The following example shows that AAA accounting has been configured for an SSL VPN session:

```
Router (config)# aaa accounting-list aaalist1
```

Related Commands

Command	Description
aaa accounting network SSLVPN start-stop group radius	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.

aaa accounting jitter maximum

To provide an interval of time between records so that the AAA server does not get overwhelmed by a constant stream of records, use the **aaa accounting jitter maximum** command in global configuration mode. To return to the default interval, use the **no** form of this command.

aaa accounting jitter maximum *max-value*

no aaa accounting jitter

Syntax Description

jitter-value	Allows the maximum jitter value from 0 to 2147483 seconds to be set in periodic accounting. The value 0 turns off jitter.

Defaults

Jitter is set to 300 seconds (5 minutes) by default.

Command Modes

Global configuration

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

If certain applications require that periodic records be sent at exact intervals, disable jitter by setting it to 0.

Examples

The following example sets the maximum jitter value to 20 seconds:

```
aaa accounting jitter maximum 20
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.

aaa accounting nested

To specify that NETWORK records be generated, or nested, within EXEC "start" and "stop" records for PPP users who start EXEC terminal sessions, use the **aaa accounting nested** command in global configuration mode. To allow the sending of records for users with a NULL username, use the **no** form of this command.

aaa accounting nested [**suppress stop**]

no aaa accounting nested [**suppress stop**]

Syntax Description

suppress stop	(Optional) Prevents sending a multiple set of records (one from EXEC and one from PPP) for the same client.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The **suppress** and **stop** keywords were added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **aaa accounting nested** command when you want to specify that NETWORK records be nested within EXEC "start" and "stop" records, such as for PPP users who start EXEC terminal sessions. In some cases, such as billing customers for specific services, is can be desirable to keep NETWORK "start" and "stop" records together, essentially nesting them within the framework of the EXEC "start" and "stop" messages. For example, if you dial in using PPP, you can create the following records: EXEC-start, NETWORK-start, EXEC-stop, and NETWORK-stop. By using the **aaa accounting nested** command to generate accounting records, NETWORK-stop records follow NETWORK-start messages: EXEC-start, NETWORK-start, NETWORK-stop, EXEC-stop.

Use the **aaa accounting nested suppress stop** command to suppress the sending of EXEC accounting records and to send only PPP accounting records.

Examples

The following example enables nesting of NETWORK accounting records for user sessions:

```
Router(config)# aaa accounting nested
```

The following example disables nesting of EXEC accounting records for user sessions:

```
Router(config)# aaa accounting nested suppress stop
```

aaa accounting redundancy

To set the Accounting, Authorization, and Authentication (AAA) platform redundancy accounting behavior, use the **aaa accounting redundancy** command in global configuration mode. To disable the accounting behavior, use the **no** form of this command.

aaa accounting redundancy {**best-effort-reuse** | **new-session**}

no aaa accounting redundancy{**best-effort-reuse** | **new-session**}

Cisco 1000 Series Router

aaa accounting redundancy {**best-effort-reuse** | **new-session** | **suppress system-records**}

no aaa accounting redundancy {**best-effort-reuse** | **new-session** | **suppress system-records**}

Syntax Description

best-effort-reuse	Specifies accounting redundant session as existing session on switchover.
new-session	Specifies accounting redundant session as a new session on switchover.
suppress	Suppresess specific records on switchover.
system-records	Generates system records on switchover

Command Default

By default, the redundant session is set as a new session on switchover.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0 (1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M
Cisco IOS XE Release 2.6	This command was integrated on Cisco IOS XE Release 2.6.

Usage Guidelines

Use the **aaa accounting redundancy** command to specify the AAA platform redundancy accounting behavior. This command also enables you to track and suppress the redundant sessions or existing sessions on switchover. You can use the no form of this command or use the **best-effort-use** or **new-session** keywords to set them to their respective accounting behaviors.

Examples

The following example shows how to set the AAA platform redundancy accounting behavior to track redundant session as existing session on switchover:

```
Router(config)# aaa accounting redundancy best-effort-reuse
```

Related Commands

Command	Description
aaa authentication dot1x	Specifies one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X
aaa accounting delay-start	Specifies delay generation of accounting "start" records until the user IP address is established.

aaa accounting resource start-stop group

To enable full resource accounting, which will generate both a "start" record at call setup and a "stop" record at call termination, use the **aaa accounting resource start-stop group** command in global configuration mode. To disable full resource accounting, use the **no** form of this command.

aaa accounting resource *method-list* **start-stop** [**broadcast**] **group** *groupname*

no aaa accounting resource *method-list* **start-stop** [**broadcast**] **group** *groupname*

Syntax Description

method-list	Method used for accounting services. Use one of the following options: • **default**: Uses the listed accounting methods that follow this argument as the default list of methods for accounting services. • *string*: Character string used to name the list of accounting methods.
broadcast	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.
groupname	Specifies the server group to be used for accounting services. The following are valid server group names: • *string*: Character string used to name a server group. • **radius**: Uses list of all RADIUS hosts. • **tacacs+**: Uses list of all TACACS+ hosts.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **aaa accounting resource start-stop group** command to send a "start" record at each call setup followed with a corresponding "stop" record at the call disconnect. There is a separate "call setup-call disconnect "start-stop" accounting record tracking the progress of the resource connection to the device, and a separate "user authentication start-stop accounting" record tracking the user management progress. These two sets of accounting records are interlinked by using a unique session ID for the call.

You may want to use this command to manage and monitor wholesale customers from one source of data reporting, such as accounting records.

Note Sending "start-stop" records for resource allocation along with user "start-stop" records during user authentication can lead to serious performance issues and is discouraged unless absolutely required.

All existing AAA accounting method list and server group options are made available to this command.

Examples

The following example shows how to configure resource accounting for "start-stop" records:

```
aaa new-model
aaa authentication login AOL group radius local
aaa authentication ppp default group radius local
aaa authorization exec AOL group radius if-authenticated
aaa authorization network default group radius if-authenticated
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius
aaa accounting resource default start-stop group radius
```

Related Commands

Command	Description
aaa accounting start-stop failure	Enables resource failure stop accounting support, which will only generate a stop record at any point prior to user authentication if a call is terminated.

aaa accounting resource stop-failure group

To enable resource failure stop accounting support, which will generate a "stop" record at any point prior to user authentication only if a call is terminated, use the **aaa accounting resource stop-failure group** command in global configuration mode. To disable resource failure stop accounting, use the **no** form of this command.

aaa accounting resource *method-list* **stop-failure** [**broadcast**] **group** *groupname*

no aaa accounting resource *method-list* **stop-failure** [**broadcast**] **group** *groupname*

Syntax Description

method-list	Method used for accounting services. Use one of the following options: • **default**: Uses the listed accounting methods that follow this argument as the default list of methods for accounting services. • *string*: Character string used to name the list of accounting methods.
broadcast	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.
groupname	Group to be used for accounting services. Use one of the following options: • *string*: Character string used to name a server group. • **radius**: Uses list of all RADIUS hosts. • **tacacs+**: Uses list of all TACACS+ hosts.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **aaa accounting resource stop-failure group** command to generate a "stop" record for any calls that do not reach user authentication; this function creates "stop" accounting records for the moment of call setup. All calls that pass user authentication will behave as before; that is, no additional accounting records will be seen.

All existing authentication, authorization, and accounting (AAA) accounting method list and server group options are made available to this command.

Examples

The following example shows how to configure "stop" accounting records from the moment of call setup:

```
aaa new-model
aaa authentication login AOL group radius local
aaa authentication ppp default group radius local
aaa authorization exec AOL group radius if-authenticated
aaa authorization network default group radius if-authenticated
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius
aaa accounting resource default stop-failure group radius
```

Related Commands

Command	Description
aaa accounting resource start-stop group	Enables full resource accounting, which will generate both a "start" record at call setup and a "stop" record at call termination.

aaa accounting send stop-record always

To generate authentication, authorization, and accounting (AAA) stop records regardless of whether a start record was sent earlier, use the **aaa accounting send stop-record always** command in global configuration mode. To stop generating the AAA stop records, use the **no** form of this command.

aaa accounting send stop-record always

no aaa accounting send stop-record always

Syntax Description

This command has no arguments or keywords.

Command Default

The stop records are not generated.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)S	This command was introduced.

Usage Guidelines

If you configure the **aaa accounting send stop-record always** command on a AAA server and Network Control Protocol (NCP) timeout occurs, then the stop record will be sent to the AAA server regardless of whether a start record was sent earlier.

Examples

The following example shows how to generate AAA stop records constantly if a start record is not sent:

```
Router> enable
Router# configure terminal
Router(config)# aaa accounting send stop-record always
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.

aaa accounting send stop-record authentication

To refine generation of authentication, authorization, and accounting (AAA) accounting "stop" records, use the **aaa accounting send stop-record authentication** command in global configuration mode. To end generation of accounting stop records, use the **no** form of this command that is appropriate.

aaa accounting send stop-record authentication {**failure** | **success remote-server**} [**vrf** *vrf-name*]

Failed Calls: End Accounting Stop Record Generation

no aaa accounting send stop-record authentication failure [**vrf** *vrf-name*]

Successful Calls: End Accounting Stop Record Generation

no aaa accounting send stop-record authentication success remote-server [**vrf** *vrf-name*]

Syntax Description

failure	Used to generate accounting "stop" records for calls that fail to authenticate at login or during session negotiation.
success	• Used to generate accounting "stop" records for calls that have been authenticated by the remote AAA server. A "stop" record will be sent after the call is terminated. • Used to generate accounting "stop" records for calls that have *not* been authenticated by the remote AAA server. A"stop" record will be sent if one of the following states is true: – The start record has been sent. – The call is successfully established and is terminated with the "stop-only" configuration.
remote-server	Used to specify that the remote server is to be used.
vrf *vrf-name*	(Optional) Used to enable this feature for a particular Virtual Private Network (VPN) routing and forwarding configuration.

Command Default

Accounting "stop" records are sent only if one of the following is true:

- A start record has been sent.
- The call is successfully established with the "stop-only" configuration and is terminated.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(1)DX	The **vrf** keyword and *vrf-name* argument were introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.

Release	Modification
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.4(2)T	The **success** and **remote-server** keywords were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

When the **aaa accounting** command is activated, by default the Cisco IOS software does not generate accounting records for system users who fail login authentication or who succeed in login authentication but fail PPP negotiation for some reason. The **aaa accounting** command can be configured to sent a "stop" record using either the **start-stop** keyword or the **stop-only** keyword.

When the **aaa accounting** command is issued with either the **start-stop** keyword or the **stop-only** keyword, the "stop" records can be further configured with the **aaa accounting send stop-record authentication** command. The failure and success keywords are mutually exclusive. If you have the **aaa accounting send stop-record authentication** command enabled with the **failure** keyword and then enable the same command with the **success** keyword, accounting stop records will no longer be generated for failed calls. Accounting stop records are sent for successful calls only until you issue either of the following commands:

- **no aaa accounting send stop-record authentication success remote-server**
- **aaa accounting send stop-record authentication failure**

When using the **failure** keyword, a "stop" record will be sent for calls that are rejected during authentication.

When using the **success** keyword, a "stop" record will be sent for calls that meet one of the following criteria:

- Calls that are authenticated by a remote AAA server when the call is terminated.
- Calls that are not authenticated by a remote AAA server and the start record has been sent.
- Calls that are successfully established and then terminated with the "stop-only" **aaa accounting** configuration.

Use the **vrf** *vrf-name* keyword and argument to generate accounting "stop" records per VPN routing and forwarding configuration.

Note The **success** and **remote-server** keywords are not available in Cisco IOS Release 12.2SX.

Examples

The following example shows how to generate "stop" records for users who fail to authenticate at login or during session negotiation:

```
aaa accounting send stop-record authentication failure
```

The following example shows "start" and "stop" records being sent for a successful call when the **aaa accounting send stop-record authentication** command is issued with the **failure** keyword:

```
Router# show running-config | include aaa
.
.
.
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting send stop-record authentication failure
aaa accounting network default start-stop group radius
.
.
.
*Jul  7 03:28:31.543: AAA/BIND(00000018): Bind i/f Virtual-Template2
*Jul  7 03:28:31.547: ppp14 AAA/AUTHOR/LCP: Authorization succeeds trivially
*Jul  7 03:28:33.555: AAA/AUTHOR (0x18): Pick method list 'default'
*Jul  7 03:28:33.555: AAA/BIND(00000019): Bind i/f
*Jul  7 03:28:33.555:  Tnl 5192 L2TP: O SCCRQ
*Jul  7 03:28:33.555:  Tnl 5192 L2TP: O SCCRQ, flg TLS, ver 2, len 141, tnl 0,
ns 0, nr 0
         C8 02 00 8D 00 00 00 00 00 00 00 80 08 00 00
         00 00 00 01 80 08 00 00 00 02 01 00 00 08 00 00
         00 06 11 30 80 10 00 00 00 07 4C 41 43 2D 74 75
         6E 6E 65 6C 00 19 00 00 00 08 43 69 73 63 6F 20
         53 79 73 74 65 6D 73 ...
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 0, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse SCCRP
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 2, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Protocol Ver 256
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 3, len 10, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Framing Cap 0x0
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 4, len 10, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Bearer Cap 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 6, len 8, flag 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Firmware Ver 0x1120
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 7, len 16, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Hostname LNS-tunnel
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 8, len 25, flag 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Vendor Name Cisco Systems, Inc.
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 9, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Assigned Tunnel ID 6897
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 10, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Rx Window Size 20050
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 11, len 22, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Chlng
         81 13 03 F6 A8 E4 1D DD 25 18 25 6E 67 8C 7C 39
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 13, len 22, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Chlng Resp
         4D 52 91 DC 1A 43 B3 31 B4 F5 B8 E1 88 22 4F 41
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: No missing AVPs in SCCRP
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: I SCCRP, flg TLS, ver 2, len 157, tnl
5192, ns 0, nr 1
contiguous pak, size 157
         C8 02 00 9D 14 48 00 00 00 00 00 01 80 08 00 00
         00 00 00 02 80 08 00 00 00 02 01 00 80 0A 00 00
         00 03 00 00 00 00 80 0A 00 00 00 04 00 00 00 00
         00 08 00 00 00 06 11 20 80 10 00 00 00 07 4C 4E
         53 2D 74 75 6E 6E 65 6C ...
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: I SCCRP from LNS-tunnel
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: O SCCCN  to LNS-tunnel tnlid 6897
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: O SCCCN, flg TLS, ver 2, len 42, tnl
6897, ns 1, nr 1
```

```
         C8 02 00 2A 1A F1 00 00 00 01 00 01 80 08 00 00
         00 00 00 03 80 16 00 00 00 0D 32 24 17 BC 6A 19
         B1 79 F3 F9 A9 D4 67 7D 9A DB
*Jul  7 03:28:33.571: uid:14 Tnl/Sn 5192/11 L2TP: O ICRQ to LNS-tunnel 6897/0
*Jul  7 03:28:33.571: uid:14 Tnl/Sn 5192/11 L2TP: O ICRQ, flg TLS, ver 2, len
63, tnl 6897, lsid 11, rsid 0, ns 2, nr 1
         C8 02 00 3F 1A F1 00 00 00 02 00 01 80 08 00 00
         00 00 00 0A 80 0A 00 00 00 0F C8 14 B4 03 80 08
         00 00 00 0E 00 0B 80 0A 00 00 00 12 00 00 00 00
         00 0F 00 09 00 64 0F 10 09 02 02 00 1B 00 00
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse  AVP 0, len 8, flag
0x8000 (M)
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse ICRP
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse  AVP 14, len 8, flag
0x8000 (M)
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Assigned Call ID 5
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: No missing AVPs in ICRP
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: I ICRP, flg TLS, ver 2, len
28, tnl 5192, lsid 11, rsid 0, ns 1, nr 3
contiguous pak, size 28
         C8 02 00 1C 14 48 00 0B 00 01 00 03 80 08 00 00
         00 00 00 0B 80 08 00 00 00 0E 00 05
*Jul  7 03:28:33.579: uid:14 Tnl/Sn 5192/11 L2TP: O ICCN to LNS-tunnel 6897/5
*Jul  7 03:28:33.579: uid:14 Tnl/Sn 5192/11 L2TP: O ICCN, flg TLS, ver 2, len
167, tnl 6897, lsid 11, rsid 5, ns 3, nr 2
         C8 02 00 A7 1A F1 00 05 00 03 00 02 80 08 00 00
         00 00 00 0C 80 0A 00 00 00 18 06 1A 80 00 00 0A
         00 00 00 26 06 1A 80 00 80 0A 00 00 00 13 00 00
         00 01 00 15 00 00 00 1B 01 04 05 D4 03 05 C2 23
         05 05 06 0A 0B E2 7A ...
*Jul  7 03:28:33.579: RADIUS/ENCODE(00000018):Orig. component type = PPoE
*Jul  7 03:28:33.579: RADIUS(00000018): Config NAS IP: 0.0.0.0
*Jul  7 03:28:33.579: RADIUS(00000018): sending
*Jul  7 03:28:33.579: RADIUS/ENCODE: Best Local IP-Address 192.168.202.169 for
Radius-Server 192.168.202.169
*Jul  7 03:28:33.579: RADIUS(00000018): Send Accounting-Request to
172.19.192.238:2196 id 1646/23, len 176
*Jul  7 03:28:33.579: RADIUS:  authenticator 3C 81 D6 C5 2B 6D 21 8E - 19 FF
43 B5 41 86 A8 A5
*Jul  7 03:28:33.579: RADIUS:  Acct-Session-Id     [44]  10  "00000023"
*Jul  7 03:28:33.579: RADIUS:  Framed-Protocol     [7]   6
PPP                      [1]
*Jul  7 03:28:33.579: RADIUS:  Tunnel-Medium-Type  [65]  6
00:IPv4                  [1]
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Client-Endpoi[66]  10  "192.168.202.169"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Server-Endpoi[67]  10  "192.168.202.169"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Assignment-Id[82]  5   "lac"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Type         [64]  6
00:L2TP                  [3]
*Jul  7 03:28:33.583: RADIUS:  Acct-Tunnel-Connecti[68]  12  "3356800003"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Client-Auth-I[90]  12  "LAC-tunnel"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Server-Auth-I[91]  12  "LNS-tunnel"
*Jul  7 03:28:33.583: RADIUS:  User-Name           [1]   16  "user@domain.com"
*Jul  7 03:28:33.583: RADIUS:  Acct-Authentic      [45]  6
Local                    [2]
*Jul  7 03:28:33.583: RADIUS:  Acct-Status-Type    [40]  6
Start                    [1]
*Jul  7 03:28:33.583: RADIUS:  NAS-Port-Type       [61]  6
Virtual                  [5]
*Jul  7 03:28:33.583: RADIUS:  NAS-Port            [5]   6
0
*Jul  7 03:28:33.583: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:28:33.583: RADIUS:  Service-Type        [6]   6
Framed                   [2]
```

```
*Jul  7 03:28:33.583: RADIUS:  NAS-IP-Address      [4]   6
192.168.202.169
*Jul  7 03:28:33.583: RADIUS:  Acct-Delay-Time     [41]  6
0
*Jul  7 03:28:33.683: RADIUS: Received from id 1646/23 192.168.202.169:2196,
Accounting-response, len 20
*Jul  7 03:28:33.683: RADIUS:  authenticator 1C E9 53 42 A2 8A 58 9A - C3 CC
1D 79 9F A4 6F 3A
```

The following example shows the "stop" record being sent when the call is rejected during authentication when the **aaa accounting send stop-record authentication** command is issued with the **success** keyword.

```
Router# show running-config | include aaa
,
,
,
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting send stop-record authentication success remote-server
aaa accounting network default start-stop group radius

Router#

*Jul  7 03:39:40.199: AAA/BIND(00000026): Bind i/f Virtual-Template2
*Jul  7 03:39:40.199: ppp21 AAA/AUTHOR/LCP: Authorization succeeds trivially
*Jul  7 03:39:42.199: RADIUS/ENCODE(00000026):Orig. component type = PPoE
*Jul  7 03:39:42.199: RADIUS:  AAA Unsupported     [156] 7
*Jul  7 03:39:42.199: RADIUS:   30 2F 30 2F
30                                  [0/0/0]
*Jul  7 03:39:42.199: RADIUS(00000026): Config NAS IP: 0.0.0.0
*Jul  7 03:39:42.199: RADIUS/ENCODE(00000026): acct_session_id: 55
*Jul  7 03:39:42.199: RADIUS(00000026): sending
*Jul  7 03:39:42.199: RADIUS/ENCODE: Best Local IP-Address 192.168.202.169 for
Radius-Server 192.168.202.169
*Jul  7 03:39:42.199: RADIUS(00000026): Send Access-Request to
172.19.192.238:2195 id 1645/14, len 94
*Jul  7 03:39:42.199: RADIUS:  authenticator A6 D1 6B A4 76 9D 52 CF - 33 5D
16 BE AC 7E 5F A6
*Jul  7 03:39:42.199: RADIUS:  Framed-Protocol     [7]   6
PPP                         [1]
*Jul  7 03:39:42.199: RADIUS:  User-Name           [1]   16  "user@domain.com"
*Jul  7 03:39:42.199: RADIUS:  CHAP-Password       [3]   19  *
*Jul  7 03:39:42.199: RADIUS:  NAS-Port-Type       [61]  6
Virtual                     [5]
*Jul  7 03:39:42.199: RADIUS:  NAS-Port            [5]   6
0
*Jul  7 03:39:42.199: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:39:42.199: RADIUS:  Service-Type        [6]   6
Framed                      [2]
*Jul  7 03:39:42.199: RADIUS:  NAS-IP-Address      [4]   6
192.168.202.169
*Jul  7 03:39:42.271: RADIUS: Received from id 1645/14 192.168.202.169:2195,
Access-Accept, len 194
*Jul  7 03:39:42.271: RADIUS:  authenticator 30 AD FF 8E 59 0C E4 6C - BA 11
23 63 81 DE 6F D7
*Jul  7 03:39:42.271: RADIUS:  Framed-Protocol     [7]   6
PPP                         [1]
*Jul  7 03:39:42.275: RADIUS:  Service-Type        [6]   6
Framed                      [2]
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  26
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   20  "vpdn:tunnel-
id=lac"
```

```
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  29
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   23  "vpdn:tunnel-
type=l2tp"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  30
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   24  "vpdn:gw-
password=cisco"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  31
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   25  "vpdn:nas-
password=cisco"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  34
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   28  "vpdn:ip-
addresses=192.168.202.169"
*Jul  7 03:39:42.275: RADIUS:  Service-Type        [6]   6
Framed                   [2]
*Jul  7 03:39:42.275: RADIUS:  Framed-Protocol     [7]   6
PPP                      [1]
*Jul  7 03:39:42.275: RADIUS(00000026): Received from id 1645/14
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: Framed-Protocol
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: service-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: tunnel-id
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: tunnel-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: gw-password
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: nas-password
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: ip-addresses
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: service-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: Framed-Protocol
*Jul  7 03:39:42.279: AAA/BIND(00000027): Bind i/f
*Jul  7 03:39:42.279:  Tnl 21407 L2TP: O SCCRQ
*Jul  7 03:39:42.279:  Tnl 21407 L2TP: O SCCRQ, flg TLS, ver 2, len 134, tnl
0, ns 0, nr 0
         C8 02 00 86 00 00 00 00 00 00 00 80 08 00 00
         00 00 00 01 80 08 00 00 00 02 01 00 00 08 00 00
         00 06 11 30 80 09 00 00 00 07 6C 61 63 00 19 00
         00 00 08 43 69 73 63 6F 20 53 79 73 74 65 6D 73
         2C 20 49 6E 63 2E 80 ...
*Jul  7 03:39:49.279:  Tnl 21407 L2TP: O StopCCN
*Jul  7 03:39:49.279:  Tnl 21407 L2TP: O StopCCN, flg TLS, ver 2, len 66, tnl
0, ns 1, nr 0
         C8 02 00 42 00 00 00 00 00 01 00 00 80 08 00 00
         00 00 00 04 80 1E 00 00 00 01 00 02 00 06 54 6F
         6F 20 6D 61 6E 79 20 72 65 74 72 61 6E 73 6D 69
         74 73 00 08 00 09 00 69 00 01 80 08 00 00 00 09
         53 9F
*Jul  7 03:39:49.279: RADIUS/ENCODE(00000026):Orig. component type = PPoE
*Jul  7 03:39:49.279: RADIUS(00000026): Config NAS IP: 0.0.0.0
*Jul  7 03:39:49.279: RADIUS(00000026): sending
*Jul  7 03:39:49.279: RADIUS/ENCODE: Best Local IP-Address 192.168.202.169 for
Radius-Server 192.168.202.169
*Jul  7 03:39:49.279: RADIUS(00000026): Send Accounting-Request to
192.168.202.169:2196 id 1646/32, len 179
*Jul  7 03:39:49.279: RADIUS:  authenticator 0A 85 2F F0 65 6F 25 E1 - 97 54
CC BF EA F7 62 89
*Jul  7 03:39:49.279: RADIUS:  Acct-Session-Id     [44]  10  "00000037"
*Jul  7 03:39:49.279: RADIUS:  Framed-Protocol     [7]   6
PPP                      [1]
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Medium-Type  [65]  6
00:IPv4                  [1]
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Client-Endpoi[66]  10  "192.168.202.169"
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Server-Endpoi[67]  10  "192.168.202.169"
*Jul  7 03:39:49.283: RADIUS:  Tunnel-Type         [64]  6
00:L2TP                  [3]
*Jul  7 03:39:49.283: RADIUS:  Acct-Tunnel-Connecti[68]  3   "0"
*Jul  7 03:39:49.283: RADIUS:  Tunnel-Client-Auth-I[90]  5   "lac"
*Jul  7 03:39:49.283: RADIUS:  User-Name           [1]   16  "user@domain.com"
```

```
*Jul  7 03:39:49.283: RADIUS:  Acct-Authentic      [45]  6
RADIUS                    [1]
*Jul  7 03:39:49.283: RADIUS:  Acct-Session-Time   [46]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Input-Octets   [42]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Output-Octets  [43]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Input-Packets  [47]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Output-Packets [48]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Terminate-Cause[49]  6   nas-
error                  [9]
*Jul  7 03:39:49.283: RADIUS:  Acct-Status-Type    [40]  6
Stop                      [2]
*Jul  7 03:39:49.283: RADIUS:  NAS-Port-Type       [61]  6
Virtual                   [5]
*Jul  7 03:39:49.283: RADIUS:  NAS-Port            [5]   6
0
*Jul  7 03:39:49.283: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:39:49.283: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:39:49.283: RADIUS:  NAS-IP-Address      [4]   6
192.168.202.169
*Jul  7 03:39:49.283: RADIUS:  Acct-Delay-Time     [41]  6
0
*Jul  7 03:39:49.335: RADIUS: Received from id 1646/32 192.168.202.169:2196,
Accounting-response, len 20
*Jul  7 03:39:49.335: RADIUS:  authenticator C8 C4 61 AF 4D 9F 78 07 - 94 2B
44 44 17 56 EC 03
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.

aaa accounting session-duration ntp-adjusted

To calculate RADIUS attribute 46, Acct-Sess-Time, on the basis of the Network Time Protocol (NTP) clock time, use the **aaa accounting session-duration ntp-adjusted** command in global configuration mode. To disable the calculation that was configured on the basis of the NTP clock time, use the **no** form of this command.

aaa accounting session-duration ntp-adjusted

no aaa accounting session-duration ntp-adjusted

Syntax Description

This command has no arguments or keywords.

Defaults

If this command is not configured, RADIUS attribute 46 is calculated on the basis of the 64-bit monotonically increasing counter, which is not NTP adjusted.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If this command is not configured, RADIUS attribute 46 can skew the session time by as much as 5 to 7 seconds for calls that have a duration of more than 24 hours. However, you may not want to configure the command for short-lived calls or if your device is up for only a short time because of the convergence time required if the session time is configured on the basis of the NTP clock time.

For RADIUS attribute 46 to reflect the NTP-adjusted time, you must configure the **ntp server** command as well as the **aaa accounting session-duration ntp-adjusted** command.

Examples

The following example shows that the attribute 46 session time is to be calculated on the basis of the NTP clock time:

```
aaa new-model
aaa authentication ppp default group radius
aaa accounting session-time ntp-adjusted
aaa accounting network default start-stop group radius
```

Related Commands

Command	Description
ntp server	Allows the software clock to be synchronized by a NTP time server.

aaa accounting suppress null-username

To prevent the Cisco IOS software from sending accounting records for users whose username string is NULL, use the **aaa accounting suppress null-username** command in global configuration mode. To allow sending records for users with a NULL username, use the **no** form of this command.

aaa accounting suppress null-username

no aaa accounting suppress null-username

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When **aaa accounting** is activated, the Cisco IOS software issues accounting records for all users on the system, including users whose username string, because of protocol translation, is NULL. This command prevents accounting records from being generated for those users who do not have usernames associated with them.

Examples

The following example suppresses accounting records for users who do not have usernames associated with them:

```
aaa accounting suppress null-username
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.

aaa accounting update

To enable periodic interim accounting records to be sent to the accounting server, use the **aaa accounting update** command in global configuration mode. To disable interim accounting updates, use the **no** form of this command.

aaa accounting update [**newinfo**] [**periodic** *number* [**jitter** {**maximum** *max-value*}]]

no aaa accounting update

Syntax Description

newinfo	(Optional) An interim accounting record is sent to the accounting server whenever there is new accounting information to report relating to the user in question.
periodic	(Optional) An interim accounting record is sent to the accounting server periodically, as defined by the *number*.
number	(Optional) Integer specifying number of minutes.
jitter	(Optional) Allows you to set the maximum jitter value in periodic accounting.
maximum *max-value*	The number of seconds to set for maximum jitter in periodic accounting. The value 0 turns off jitter. Jitter is set to 300 seconds (5 minutes) by default.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(13)T	Introduced support for generation of an additional updated interim accounting record that contains all available attributes when a call leg is connected.
12.2(15)T11	The **jitter** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

- When the **aaa accounting update** command is activated, the Cisco IOS software issues interim accounting records for all users on the system. If the **newinfo** keyword is used, interim accounting records will be sent to the accounting server every time there is new accounting information to report. An example would be when IP Control Protocol (IPCP) completes IP address negotiation with the remote peer. The interim accounting record will include the negotiated IP address used by the remote peer.

- When the **gw-accounting aaa** command and the **aaa accounting update newinfo** command and keyword are activated, Cisco IOS software generates and sends an additional updated interim accounting record to the accounting server when a call leg is connected. All attributes (for example, h323-connect-time and backward-call-indicators (BCI)) available at the time of call connection are sent through this interim updated accounting record.
- When used with the **periodic** keyword, interim accounting records are sent periodically as defined by the number. The interim accounting record contains all of the accounting information recorded for that user up to the time the accounting record is sent.
- When using both the **newinfo** and **periodic** keywords, interim accounting records are sent to the accounting server every time there is new accounting information to report, and accounting records are sent to the accounting server periodically as defined by the number. For example, if you configure the **aaa accounting update newinfo periodic** *number* command, all users currently logged in will continue to generate periodic interim accounting records while new users will generate accounting records based on the **newinfo** algorithm.
- Vendor-specific attributes (VSAs) such as h323-connect-time and backward-call-indicator (BCI) are transmitted in the interim update RADIUS message when the **aaa accounting update newinfo** command and keyword are enabled.
- Jitter is used to provide an interval of time between records so that the AAA server does not get overwhelmed by a constant stream of records. If certain applications require that periodic records be sent a exact intervals, you should disable jitter by setting it to 0.

Caution Using the **aaa accounting update periodic** command and keyword can cause heavy congestion when many users are logged into the network.

Examples

The following example sends PPP accounting records to a remote RADIUS server. When IPCP completes negotiation, this command sends an interim accounting record to the RADIUS server that includes the negotiated IP address for this user; it also sends periodic interim accounting records to the RADIUS server at 30-minute intervals.

```
aaa accounting network default start-stop group radius
aaa accounting update newinfo periodic 30
```

The following example sends periodic interim accounting records to the RADIUS server at 30-minute intervals and disables jitter:

```
aaa accounting update newinfo periodic 30 jitter maximum 0
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
gw-accounting aaa	Enables VoIP gateway accounting through the AAA system.

aaa attribute

To add calling line identification (CLID) and dialed number identification service (DNIS) attribute values to a user profile, use the **aaa attribute** command in AAA-user configuration mode. To remove this command from your configuration, use the **no** form of this command.

aaa attribute {**clid** | **dnis**} *attribute-value*

no aaa attribute {**clid** | **dnis**} *attribute-value*

Syntax Description

clid	Adds CLID attribute values to the user profile.
dnis	Adds DNIS attribute values to the user profile.
attribute-value	Specifies a name for CLID or DNIS attribute values.

Command Default

If this command is not enabled, you will have an empty user profile.

Command Modes

AAA-user configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Use the **aaa attribute** command to add CLID or DNIS attribute values to a named user profile, which is created by using the **aaa user profile** command. The CLID or DNIS attribute values can be associated with the record that is going out with the user profile (via the **test aaa group** command), thereby providing the RADIUS server with access to CLID or DNIS information when the server receives a RADIUS record.

Examples

The following example shows how to add CLID and DNIS attribute values to the user profile “cat”:

```
aaa user profile cat
 aaa attribute clid clidval
 aaa attribute dnis dnisval
```

Related Commands

Command	Description
aaa user profile	Creates a AAA user profile.
test aaa group	Associates a DNIS or CLID user profile with the record that is sent to the RADIUS server.

aaa attribute list

To define an authentication, authorization, and accounting (AAA) attribute list locally on a router, use the **aaa attribute list** command in global configuration mode. To remove the AAA attribute list, use the **no** form of this command.

aaa attribute list *list-name*

no aaa attribute list *list-name*

Syntax Description

list-name	Name of the local attribute list.

Command Default

A local attribute list is not defined.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)XI1	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

There is no limit to the number of lists that can be defined (except for NVRAM storage limits).

Examples

The following example shows that the attribute list named “TEST” is to be added to the subscriber profile “cisco.com”:

```
aaa authentication ppp template1 local
aaa authorization network template1 local
!
aaa attribute list TEST
   attribute type interface-config "ip unnumbered FastEthernet0" service ppp protocol lcp
   attribute type interface-config "ip vrf forwarding blue" service ppp protocol lcp
!
ip vrf blue
 description vrf blue template1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
subscriber authorization enable
!
```

```
subscriber profile cisco.com
 service local
 aaa attribute list TEST
!
bba-group pppoe grp1
 virtual-template 1
 service profile cisco.com
!
interface Virtual-Template1
 no ip address
 no snmp trap link-status
 no peer default ip address
 no keepalive
 ppp authentication pap template1
 ppp authorization template1
!
```

Related Commands

Command	Description
attribute type	Defines an attribute type that is to be added to an attribute list locally on a router.

aaa authentication (IKEv2 profile)

To specify the AAA authentication list for Extensible Authentication Protocol (EAP) authentication, use the **aaa authentication** command in IKEv2 profile configuration mode. To remove the AAA authentication for EAP, use the **no** form of this command.

aaa authentication eap *list-name*

no aaa authentication eap

Syntax Description

eap	Specifies the external EAP server for the authentication list.
list-name	Name of the AAA authentication list.

Command Default

AAA authentication for EAP is not specified.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.1(3)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to specify the AAA authentication list for EAP authentication. The **crypto ikev2 profile** command must be enabled before this command is executed.

Examples

The following example shows how to configure the remote access server using the remote EAP authentication method with an external EAP server:

```
Router(config)# aaa new-model
Router(config)# aaa authentication login aaa-eap-list default group radius
Router(config)# crypto ikev2 profile profile2
Router(config-ikev2-profile)# authentication remote eap
Router(config-ikev2-profile)# aaa authentication eap aaa-eap-list
```

The following example shows how to configure the remote access server using the remote EAP authentication method with a local and external EAP server:

```
Router(config)# aaa new-model
Router(config)# aaa authentication login aaa-eap-list default group radius
Router(config)# aaa authentication login aaa-eap-local-list default group tacacs
Router(config)# crypto ikev2 profile profile2
Router(config-ikev2-profile)# authentication remote eap
Router(config-ikev2-profile)# authentication remote eap-local
Router(config-ikev2-profile)# aaa authentication eap aaa-eap-list
Router(config-ikev2-profile)# aaa authentication eap-local aaa-eap-local-list
```

Related Commands

Command	Description
crypt ikev2 profile	Defines an IKEv2 profile.

aaa authentication (WebVPN)

To configure authentication, authorization, and accounting (AAA) authentication for SSL VPN sessions, use the **aaa authentication** command in webvpn context configuration mode. To remove the AAA configuration from the SSL VPN context configuration, use the **no** form of this command.

aaa authentication {**domain** *name* | **list** *name*}

no aaa authentication {**domain** | **list**}

Syntax Description

domain *name*	Configures authentication using the specified domain name.
list *name*	Configures authentication using the specified list name.

Command Default

If this command is not configured or if the **no** form of this command is entered, the SSL VPN gateway will use global AAA parameters (if configured).

Command Modes

Webvpn context configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The **aaa authentication** command is entered to specify an authentication list or server group under a SSL VPN context configuration. If this command is not configured and AAA is configured globally on the router, global authentication will be applied to the context configuration.

The database that is configured for remote-user authentication on the SSL VPN gateway can be a local database, or the database can be accessed through any RADIUS or TACACS+ AAA server.

We recommend that you use a separate AAA server, such as a Cisco Access Control Server (ACS). A separate AAA server provides a more robust security solution. It allows you to configure unique passwords for each remote user and accounting and logging for remote-user sessions.

Examples

Local AAA Example (Default to Global Configuration)

The following example configures local AAA for remote-user connections. Notice that the **aaa authentication** command is not configured in a context configuration.

```
Router (config)# aaa new-model
Router (config)# username USER1 secret 0 PsW2143
Router (config)# aaa authentication login default local
```

AAA Access Control Server Example

The following example configures a RADIUS server group and associates the AAA configuration under the SSL VPN context configuration.

```
Router (config)# aaa new-model
Router (config)# aaa group server radius myServer
Router (config-sg-radius)# server 10.1.1.20 auth-port 1645 acct-port 1646
Router (config-sg-radius)# exit
Router (config)# aaa authentication login default local group myServer
Router (config)# radius-server host 10.1.1.0 auth-port 1645 acct-port 1646
Router (config)# webvpn context context1
Router (config-webvpn-context)# aaa authentication list myServer
Router (config-webvpn-context)# exit
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

aaa authentication arap

To enable an authentication, authorization, and accounting (AAA) authentication method for AppleTalk Remote Access (ARA), use the **aaa authentication arap** command in global configuration mode. To disable this authentication, use the **no** form of this command.

aaa authentication arap {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication arap {**default** | *list-name*} *method1* [*method2*...]

Syntax Description

default	Uses the listed methods that follow this argument as the default list of methods when a user logs in.
list-name	Character string used to name the following list of authentication methods tried when a user logs in.
method1 [*method2*...]	At least one of the keywords described in Table 2.

Defaults

If the **default** list is not set, only the local user database is checked. This has the same effect as the following command:

```
aaa authentication arap default local
```

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	Group server and local-case support were added as method keywords for this command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The list names and default that you set with the **aaa authentication arap** command are used with the **arap authentication** command. Note that ARAP guest logins are disabled by default when you enable AAA. To allow guest logins, you must use either the **guest** or **auth-guest** method listed in Table 2. You can only use one of these methods; they are mutually exclusive.

Create a list by entering the **aaa authentication arap** *list-name method* command, where *list-name* is any character string used to name this list (such as *MIS-access*). The *method* argument identifies the list of methods the authentication algorithm tries in the given sequence. See Table 2 for descriptions of method keywords.

To create a default list that is used if no list is specified in the **arap authentication** command, use the **default** keyword followed by the methods you want to be used in default situations.

The additional methods of authentication are used only if the previous method returns an error, not if it fails.

Use the **more system:running-config** command to view currently configured lists of authentication methods.

Note In Table 2, the **group radius**, **group tacacs+**, and **group** *group-name* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs+-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Table 2 aaa authentication arap Methods

Keyword	Description
guest	Allows guest logins. This method must be the first method listed, but it can be followed by other methods if it does not succeed.
auth-guest	Allows guest logins only if the user has already logged in to EXEC. This method must be the first method listed, but can be followed by other methods if it does not succeed.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command.

Examples

The following example creates a list called *MIS-access*, which first tries TACACS+ authentication and then none:

```
aaa authentication arap MIS-access group tacacs+ none
```

The following example creates the same list, but sets it as the default list that is used for all ARA protocol authentications if no other list is specified:

```
aaa authentication arap default group tacacs+ none
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.

aaa authentication attempts login

To set the maximum number of login attempts that will be permitted before a session is dropped, use the **aaa authentication attempts login** command in global configuration mode. To reset the number of attempts to the default, use the **no** form of this command.

aaa authentication attempts login *number-of-attempts*

no aaa authentication attempts login

Syntax Description

number-of-attempts	Number of login attempts. Range is from 1 to 25. Default is 3.

Defaults

3 attempts

Command Modes

Global configuration

Command History

Release	Modification
12.2 T	This command was introduced.

Usage Guidelines

The **aaa authentication attempts login** command configures the number of times a router will prompt for username and password before a session is dropped.

The **aaa authentication attempts login** command can be used only if the **aaa new-model** command is configured.

Examples

The following example configures a maximum of 5 attempts at authentication for login:

```
aaa authentication attempts login 5
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.

aaa authentication auto (WebVPN)

To allow automatic authentication for Secure Socket Layer virtual private network (SSL VPN) users, use the **aaa authentication auto** command in webvpn context configuration mode. To disable automatic authentication, use the **no** form of this command.

aaa authentication auto

no aaa authentication auto

Syntax Description

This command has no arguments or keywords.

Command Default

Automatic authentication is not allowed.

Command Modes

Webvpn context (config-webvpn-context)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Configuring this command allows users to provide their usernames and passwords via the gateway page URL. They do not have to enter the usernames and passwords again from the login page.

A user can embed his or her username and password in the URL using the following format:

```
http://<gateway-address>/<vw_context>/webvpnauth?username:password
```

Examples

The following example shows that automatic authentication has been configured for users:

```
Router (config)# webvpn context
Router (config-webvpn-context)# aaa authentication auto
```

aaa authentication banner

To configure a personalized banner that will be displayed at user login, use the **aaa authentication banner** command in global configuration mode. To remove the banner, use the **no** form of this command.

aaa authentication banner *dstringd*

no aaa authentication banner

Syntax Description

d	Any delimiting character at the beginning and end of the *string* that notifies the system that the *string* is to be displayed as the banner. The delimiting character can be any character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.
string	Any group of characters, excluding the one used as the delimiter. The maximum number of characters that you can display is 2996.

Defaults

Not enabled

Command Modes

Global configuration

Command History

Release	Modification
11.3(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **aaa authentication banner** command to create a personalized message that appears when a user logs in to the system. This message or banner will replace the default message for user login.

To create a login banner, you need to configure a delimiting character, which notifies the system that the following text string is to be displayed as the banner, and then the text string itself. The delimiting character is repeated at the end of the text string to signify the end of the banner. The delimiting character can be any character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.

Note The AAA authentication banner message is not displayed if TACACS+ is the first method in the method list.

Examples

The following example shows the default login message if **aaa authentication banner** is not configured. (RADIUS is specified as the default login authentication method.)

```
aaa new-model
aaa authentication login default group radius
```

This configuration produces the following standard output:

```
User Verification Access
Username:
Password:
```

The following example configures a login banner (in this case, the phrase "Unauthorized use is prohibited.") that will be displayed when a user logs in to the system. In this case, the asterisk (*) symbol is used as the delimiter. (RADIUS is specified as the default login authentication method.)

```
aaa new-model
aaa authentication banner *Unauthorized use is prohibited.*
aaa authentication login default group radius
```

This configuration produces the following login banner:

```
Unauthorized use is prohibited.
Username:
```

Related Commands

Command	Description
aaa authentication fail-message	Configures a personalized banner that will be displayed when a user fails login.

aaa authentication dot1x

To specify one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X, use the **aaa authentication dot1x** command in global configuration mode. To disable authentication, use the **no** form of this command

aaa authentication dot1x {**default** | **listname**} *method1* [*method2...*]

no aaa authentication dot1x {**default** | **listname**} *method1* [*method2...*]

Syntax Description

default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
listname	Character string used to name the list of authentication methods tried when a user logs in.
method1 [*method2...*]	At least one of these keywords: • **enable**—Uses the enable password for authentication. • **group radius**—Uses the list of all RADIUS servers for authentication. • **line**—Uses the line password for authentication. • **local**—Uses the local username database for authentication. • **local-case**—Uses the case-sensitive local username database for authentication. • **none**—Uses no authentication. The client is automatically authenticated by the switch without using the information supplied by the client.

Defaults

No authentication is performed.

Command Types

Global configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced for the Cisco Ethernet switch network module.
12.2(15)ZJ	This command was implemented on the following platforms for the Cisco Ethernet Switch Module: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series.
12.3(2)XA	This command was introduced on the following Cisco router platforms: Cisco 806, Cisco 831, Cisco 836, Cisco 837, Cisco 1701, Cisco 1710, Cisco 1721, Cisco 1751-V, and Cisco 1760.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T. Router support was added for the following platforms: Cisco 1751, Cisco 2610XM – Cisco 2611XM, Cisco 2620XM – Cisco 2621XM, Cisco 2650XM – Cisco 2651XM, Cisco 2691, Cisco 3640, Cisco 3640A, and Cisco 3660.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The *method* argument identifies the list of methods that the authentication algorithm tries in the given sequence to validate the password provided by the client. The only method that is truly 802.1X-compliant is the **group radius** method, in which the client data is validated against a RADIUS authentication server. The remaining methods enable AAA to authenticate the client by using locally configured data. For example, the **local** and **local-case** methods use the username and password that are saved in the Cisco IOS configuration file. The **enable** and **line** methods use the **enable** and **line** passwords for authentication.

If you specify **group radius**, you must configure the RADIUS server by entering the **radius-server host** global configuration command. If you are not using a RADIUS server, you can use the **local** or **local-case** methods, which access the local username database to perform authentication. By specifying the **enable** or **line** methods, you can supply the clients with a password to provide access to the switch.

Use the **show running-config** privileged EXEC command to display the configured lists of authentication methods.

Examples

The following example shows how to enable AAA and how to create an authentication list for 802.1X. This authentication first tries to contact a RADIUS server. If this action returns an error, the user is allowed access with no authentication:

```
Router(config)# aaa new model
Router(config)# aaa authentication dot1x default group radius none
```

Related Commands

Command	Description
debug dot1x	Displays 802.1X debugging information.
identity profile default	Creates an identity profile and enters dot1x profile configuration mode.
show dot1x	Displays details for an identity profile.
show dot1x (EtherSwitch)	Displays 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.

aaa authentication enable default

To enable authentication, authorization, and accounting (AAA) authentication to determine whether a user can access the privileged command level, use the **aaa authentication enable default** command in global configuration mode. To disable this authorization method, use the **no** form of this command.

aaa authentication enable default *method1* [*method2*...]

no aaa authentication enable default *method1* [*method2*...]

Syntax Description

method1 [*method2*...]	At least one of the keywords described in Table 3.

Defaults

If the **default** list is not set, only the enable password is checked. This has the same effect as the following command:

```
aaa authentication enable default enable
```

On the console, the enable password is used if it exists. If no password is set, the process will succeed anyway.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	Group server support was added as various method keywords for this command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **aaa authentication enable default** command to create a series of authentication methods that are used to determine whether a user can access the privileged command level. Method keywords are described in Table 3. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify **none** as the final method in the command line.

All **aaa authentication enable default** requests sent by the router to a RADIUS server include the username "$enab15$."

Note An enable authentication request for $enab{*x*}$ is sent only for RADIUS servers.

If a default authentication routine is not set for a function, the default is **none** and no authentication is performed. Use the **more system:running-config** command to view currently configured lists of authentication methods.

Note In Table 3, the **group radius**, **group tacacs+**, and **group** *group-name* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs+-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Table 3 aaa authentication enable default Methods

Keyword	Description
enable	Uses the enable password for authentication. **Note** An authentication request fails over to the next authentication method only if no enable password is configured on the router.
line	Uses the line password for authentication.
none	Uses no authentication.
group radius	Uses the list of all RADIUS servers for authentication. **Note** The RADIUS method does not work on a per-username basis.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command.

Examples

The following example shows how to create an authentication list that first tries to contact a TACACS+ server. If no server can be found, AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication.

```
aaa authentication enable default group tacacs+ enable none
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict network access to a user.
aaa new-model	Enables the AAA access control model.
enable password	Sets a local password to control access to various privilege levels.

aaa authentication eou default enable group radius

To set authentication lists for Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP), use the **aaa authentication eou default enable group radius** command in global configuration mode. To remove the authentication lists, use the **no** form of this command.

aaa authentication eou default enable group radius

no aaa authentication eou default enable group radius

Syntax Description

This command has no arguments or keywords.

Defaults

Authentication lists for EAPoUDP are not set.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Examples

The following example shows that authentication lists have been set for EAPoUDP:

```
Router (config)# aaa new-model
Router (config)# aaa authentication eou default enable group radius
```

Related Commands

Command	Description
eou	Provides information about EAPoUDP.
ip admission	Creates a Layer 3 network admission control rule to be applied to the interface.

aaa authentication fail-message

To configure a personalized banner that will be displayed when a user fails login, use the **aaa authentication fail-message** command in global configuration mode. To remove the failed login message, use the **no** form of this command.

aaa authentication fail-message *dstringd*

no aaa authentication fail-message

Syntax Description

d	The delimiting character at the beginning and end of the *string* that notifies the system that the *string* is to be displayed as the banner. The delimiting character can be any character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.
string	Any group of characters, excluding the one used as the delimiter. The maximum number of characters that you can display is 2996.

Defaults

Not enabled

Command Modes

Global configuration

Command History

Release	Modification
11.3(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **aaa authentication fail-message** command to create a personalized message that appears when a user fails login. This message will replace the default message for failed login.

To create a failed-login banner, you need to configure a delimiting character, which notifies the system that the following text string is to be displayed as the banner, and then the text string itself. The delimiting character is repeated at the end of the text string to signify the end of the banner. The delimiting character can be any character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.

Examples

The following example shows the default login message and failed login message that is displayed if **aaa authentication banner** and **aaa authentication fail-message** are not configured. (RADIUS is specified as the default login authentication method.)

```
aaa new-model
aaa authentication login default group radius
```

This configuration produces the following standard output:

```
User Verification Access
Username:
Password:

% Authentication failed.
```

The following example configures both a login banner (“Unauthorized use is prohibited.”) and a login-fail message (“Failed login. Try again.”). The login message will be displayed when a user logs in to the system. The failed-login message will display when a user tries to log in to the system and fails. (RADIUS is specified as the default login authentication method.) In this example, the asterisk (*) is used as the delimiting character.

```
aaa new-model
aaa authentication banner *Unauthorized use is prohibited.*
aaa authentication fail-message *Failed login. Try again.*
aaa authentication login default group radius
```

This configuration produces the following login and failed login banner:

```
Unauthorized use is prohibited.
Username:
Password:
Failed login. Try again.
```

Related Commands

Command	Description
aaa authentication banner	Configures a personalized banner that will be displayed at user login.

aaa authentication login

To set authentication, authorization, and accounting (AAA) authentication at login, use the **aaa authentication login** command in global configuration mode. To disable AAA authentication, use the **no** form of this command.

aaa authentication login {**default** | *list-name*} {[**passwd-expiry**] *method1* [*method2*...]}

no aaa authentication login {**default** | *list-name*} {[**passwd-expiry**] *method1* [*method2*...]}

Syntax Description

default	Uses the listed authentication methods that follow this keyword as the default list of methods when a user logs in.
list-name	Character string used to name the list of authentication methods activated when a user logs in. See the "Authentication Methods That Cannot Be Used for the list-name Argument" in the "Usage Guidelines" section for more information.
passwd-expiry	Enables password aging on a local authentication list. **Note** The **radius-server vsa send authentication** command is required to make the **passwd-expiry** keyword work.
method1 [*method2*...]	The list of methods that the authentication algorithm tries in the given sequence. You must enter at least one method; you may enter up to four methods. Method keywords are described in Table 4.

Command Default

AAA authentication at login is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	This command was modified. The **group radius**, **group tacacs+**, and **local-case** keywords were added as methods for authentication.
12.4(6)T	This command was modified. The **password-expiry** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB. The **cache** *group-name* keyword and argument were added as a method for authentication.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.1(1)T	This command was modified. The **group ldap** keyword was added.

Release	Modification
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

If the **default** keyword is not set, only the local user database is checked. This has the same effect as the following command:

```
aaa authentication login default local
```

Note On the console, login will succeed without any authentication checks if **default** keyword is not set.

The default and optional list names that you create with the **aaa authentication login** command are used with the **login authentication** command.

Create a list by entering the **aaa authentication login** *list-name method* command for a particular protocol. The *list-name* argument is the character string used to name the list of authentication methods activated when a user logs in. The *method* argument identifies the list of methods that the authentication algorithm tries, in the given sequence. The "Authentication Methods That Cannot Be Used for the list-name Argument" section lists authentication methods that cannot be used for the *list-name* argument and Table 4 describes the method keywords.

To create a default list that is used if no list is assigned to a line, use the **login authentication** command with the default argument followed by the methods you want to use in default situations.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

If authentication is not specifically set for a line, the default is to deny access and no authentication is performed. Use the **more system:running-config** command to display currently configured lists of authentication methods.

Authentication Methods That Cannot Be Used for the list-name Argument

The authentication methods that cannot be used for the *list-name* argument are as follows:

- **auth-guest**
- **enable**
- **guest**
- **if-authenticated**
- **if-needed**
- **krb5**
- **krb-instance**
- **krb-telnet**
- **line**
- **local**
- **none**
- **radius**

- **rcmd**
- **tacacs**
- **tacacsplus**

Note In Table 4, the **group radius**, **group tacacs+**, **group ldap**, and **group** *group-name* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the host servers. Use the **aaa group server radius**, **aaa group server ldap**, and **aaa group server tacacs+** commands to create a named group of servers.

Table 4 describes the method keywords.

Table 4 aaa authentication login Methods Keywords

Keyword	Description
cache *group-name*	Uses a cache server group for authentication.
enable	Uses the enable password for authentication. This keyword cannot be used.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command.
group ldap	Uses the list of all Lightweight Directory Access Protocol (LDAP) servers for authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
krb5	Uses Kerberos 5 for authentication.
krb5-telnet	Uses Kerberos 5 Telnet authentication protocol when using Telnet to connect to the router.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.
passwd-expiry	Uses the login list to provide password aging support.

Examples

The following example shows how to create an AAA authentication list called *MIS-access*. This authentication first tries to contact a TACACS+ server. If no server is found, TACACS+ returns an error and AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication.

```
aaa authentication login MIS-access group tacacs+ enable none
```

The following example shows how to create the same list, but it sets it as the default list that is used for all login authentications if no other list is specified:

```
aaa authentication login default group tacacs+ enable none
```

The following example shows how to set authentication at login to use the Kerberos 5 Telnet authentication protocol when using Telnet to connect to the router:

```
aaa authentication login default krb5
```

The following example shows how to configure password aging by using AAA with a crypto client:

```
aaa authentication login userauthen passwd-expiry group radius
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
login authentication	Enables AAA authentication for logins.

aaa authentication nasi

To specify authentication, authorization, and accounting (AAA) authentication for Netware Asynchronous Services Interface (NASI) clients connecting through the access server, use the **aaa authentication nasi** command in global configuration mode. To disable authentication for NASI clients, use the **no** form of this command.

aaa authentication nasi {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication nasi {**default** | *list-name*} *method1* [*method2*...]

Syntax Description

default	Makes the listed authentication methods that follow this argument the default list of methods used when a user logs in.
list-name	Character string used to name the list of authentication methods activated when a user logs in.
method1 [*method2*...]	At least one of the methods described in Table 5.

Defaults

If the **default** list is not set, only the local user database is selected. This has the same effect as the following command:

```
aaa authentication nasi default local
```

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.0(5)T	Group server support and **local-case** were added as method keywords for this command.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline releases or in Technology-based (T-train) releases. It might continue to appear in 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The default and optional list names that you create with the **aaa authentication nasi** command are used with the **nasi authentication** command.

Create a list by entering the **aaa authentication nasi** command, where *list-name* is any character string that names the list (such as *MIS-access*). The *method* argument identifies the list of methods the authentication algorithm tries in the given sequence. Method keywords are described in Table 5.

To create a default list that is used if no list is assigned to a line with the **nasi authentication** command, use the default argument followed by the methods that you want to use in default situations.

The remaining methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

If authentication is not specifically set for a line, the default is to deny access and no authentication is performed. Use the **more system:running-config** command to display currently configured lists of authentication methods.

Note In Table 5, the **group radius**, **group tacacs+**, and **group** *group-name* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs+-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Table 5 aaa authentication nasi Methods

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command.

Examples

The following example creates an AAA authentication list called *list1*. This authentication first tries to contact a TACACS+ server. If no server is found, TACACS+ returns an error and AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication.

```
aaa authentication nasi list1 group tacacs+ enable none
```

The following example creates the same list, but sets it as the default list that is used for all login authentications if no other list is specified:

```
aaa authentication nasi default group tacacs+ enable none
```

Related Commands

Command	Description
ip trigger-authentication (global)	Enables the automated part of double authentication at a device.
ipx nasi-server enable	Enables NASI clients to connect to asynchronous devices attached to a router.
nasi authentication	Enables AAA authentication for NASI clients connecting to a router.

Command	Description
show ipx nasi connections	Displays the status of NASI connections.
show ipx spx-protocol	Displays the status of the SPX protocol stack and related counters.

aaa authentication password-prompt

To change the text displayed when users are prompted for a password, use the **aaa authentication password-prompt** command in global configuration mode. To return to the default password prompt text, use the **no** form of this command.

aaa authentication password-prompt *text-string*

no aaa authentication password-prompt *text-string*

Syntax Description

text-string	String of text that will be displayed when the user is prompted to enter a password. If this text-string contains spaces or unusual characters, it must be enclosed in double-quotes (for example, “Enter your password:”).

Defaults

There is no user-defined *text-string*, and the password prompt appears as “Password.”

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **aaa authentication password-prompt** command to change the default text that the Cisco IOS software displays when prompting a user to enter a password. This command changes the password prompt for the enable password as well as for login passwords that are not supplied by remote security servers. The **no** form of this command returns the password prompt to the default value:

```
Password:
```

The **aaa authentication password-prompt** command does not change any dialog that is supplied by a remote TACACS+ server.

The **aaa authentication password-prompt** command works when RADIUS is used as the login method. The password prompt that is defined in the command will be shown even when the RADIUS server is unreachable. The **aaa authentication password-prompt** command does not work with TACACS+. TACACS+ supplies the network access server (NAS) with the password prompt to display to the users. If the TACACS+ server is reachable, the NAS gets the password prompt from the server and uses that prompt instead of the one defined in the **aaa authentication password-prompt** command. If the TACACS+ server is not reachable, the password prompt that is defined in the **aaa authentication password-prompt** command may be used.

Examples

The following example changes the text for the password prompt:

```
aaa authentication password-prompt "Enter your password now:"
```

Related Commands

Command	Description
aaa authentication username-prompt	Changes the text displayed when users are prompted to enter a username.
aaa new-model	Enables the AAA access control model.
enable password	Sets a local password to control access to various privilege levels.

aaa authentication ppp

To specify one or more authentication, authorization, and accounting (AAA) methods for use on serial interfaces that are running PPP, use the **aaa authentication ppp** command in global configuration mode. To disable authentication, use the **no** form of this command.

aaa authentication ppp {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication ppp {**default** | *list-name*} *method1* [*method2*...]

Syntax Description

default	Uses the listed authentication methods that follow this keyword as the default list of methods when a user logs in.
list-name	Character string used to name the list of authentication methods tried when a user logs in.
method1 [*method2*...]	Identifies the list of methods that the authentication algorithm tries in the given sequence. You must enter at least one method; you may enter up to four methods. Method keywords are described in Table 6.

Command Default

AAA authentication methods on serial interfaces running PPP are not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	Group server support and **local-case** were added as method keywords.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

If the **default** list is not set, only the local user database is checked. This has the same effect as that created by the following command:

```
aaa authentication ppp default local
```

The lists that you create with the **aaa authentication ppp** command are used with the **ppp authentication** command. These lists contain up to four authentication methods that are used when a user tries to log in to the serial interface.

Create a list by entering the **aaa authentication ppp** *list-name method* command, where *list-name* is any character string used to name this list MIS-access. The *method* argument identifies the list of methods that the authentication algorithm tries in the given sequence. You can enter up to four methods. Method keywords are described in Table 6.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to have authentication succeed even if all methods return an error.

If authentication is not specifically set for a function, the default is **none** and no authentication is performed. Use the **more system:running-config** command to display currently configured lists of authentication methods.

Note In Table 6, the **group radius**, **group tacacs+**, and **group** *group-name* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Table 6 aaa authentication ppp Methods

Keyword	Description
cache *group-name*	Uses a cache server group for authentication.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
if-needed	Does not authenticate if the user has already been authenticated on a tty line.
krb5	Uses Kerberos 5 for authentication (can be used only for Password Authentication Protocol [PAP] authentication).
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.

Cisco 10000 Series Router

The Cisco 10000 series router supports a maximum of 2,000 AAA method lists. If you configure more than 2,000 AAA method lists, traceback messages appear on the console.

Examples

The following example creates an AAA authentication list called MIS-access for serial lines that use PPP. This authentication first tries to contact a TACACS+ server. If this action returns an error, the user is allowed access with no authentication.

```
aaa authentication ppp MIS-access group tacacs+ none
```

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
aaa group server tacacs+	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
more system:running-config	Displays the contents of the currently running configuration file, the configuration for a specific interface, or map class information.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
radius-server host	Specifies a RADIUS server host.
tacacs-server host	Specifies a TACACS host.

aaa authentication sgbp

To specify one or more authentication, authorization, and accounting (AAA) authentication methods for Stack Group Bidding Protocol (SGBP), use the **aaa authentication sgbp** command in global configuration mode. To disable SGBP authentication and return to the default, use the **no** form of this command.

aaa authentication sgbp {**default** | *list-name*} *method1* [*method2...*]

no aaa authentication sgbp {**default** | *list-name*} *method1* [*method2...*]

Syntax Description

default	Uses the listed authentication methods that follow this keyword as the default list of methods when a user logs in.
list-name	Character string used to name the list of authentication methods tried when a user logs in.
method1 [*method2...*]	Identifies the list of methods that the authentication algorithm tries in the given sequence. You must enter at least one method; you may enter up to four methods. Method keywords are described in

Defaults

The **aaa authentication ppp default** command. If the **aaa authentication ppp default** command is not enabled, local authentication will be the default functionality.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command introduced.

Usage Guidelines

The lists that you create with the **aaa authentication sgbp** command are used with the **sgbp aaa authentication** command.

Create a list by entering the **aaa authentication sgbp** *list-name method* command, where the *list-name* argument is any character string used to name this list. The *method* argument identifies the list of methods that the authentication algorithm tries in the given sequence. You can enter up to four methods. Method keywords are described in Table 7.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to have authentication succeed even if all methods return an error.

Use the **more system:running-config** command to display currently configured lists of authentication methods.

Table 7 aaa authentication sgbp Methods

Keyword	Description
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command.

Examples

The following example shows how to create a AAA authentication list called SGBP. The user first tries to contact a RADIUS server for authentication. If this action returns an error, the user will try to access the local database.

```
Router(config)# aaa authentication sgbp SGBP group radius local
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP.
sgbp aaa authentication	Enables a SGBP authentication list.

aaa authentication suppress null-username

To configure Cisco IOS software to prevent an Access Request with a blank username from being sent to the RADIUS server, use the **aaa authentication suppress null-username** command in global configuration mode.

To configure Cisco IOS software to allow an Access Request with a blank username to be sent to the RADIUS server, use the **no** form of this command:

aaa authentication suppress null-username

no aaa authentication suppress null-username

SyntaxDescription

Enables the prevention of an Access Request with a blank username from being sent to the RADIUS server.

Command Default

The command-level default is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS Release 12.2(33)SRD	This command was introduced.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4

Usage Guidelines

This command ensures that unnecessary RADIUS server interaction is avoided, and RADIUS logs are kept short.

Examples

The following example shows how the **aaa authentication suppress null-username** is configured:

```
enable
configure terminal
aaa new-model
aaa authentication suppress null-username
```

Related Commands

Command	Description
aaa new-model	Enables AAA globally.

aaa authentication username-prompt

To change the text displayed when users are prompted to enter a username, use the **aaa authentication username-prompt** command in global configuration mode. To return to the default username prompt text, use the **no** form of this command.

aaa authentication username-prompt *text-string*

no aaa authentication username-prompt *text-string*

Syntax Description

text-string	String of text that will be displayed when the user is prompted to enter a username. If this text-string contains spaces or unusual characters, it must be enclosed in double-quotes (for example, “Enter your name:”).

Defaults

There is no user-defined *text-string*, and the username prompt appears as “Username.”

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **aaa authentication username-prompt** command to change the default text that the Cisco IOS software displays when prompting a user to enter a username. The **no** form of this command returns the username prompt to the default value:

```
Username:
```

Some protocols (for example, TACACS+) have the ability to override the use of local username prompt information. Using the **aaa authentication username-prompt** command will not change the username prompt text in these instances.

Note The **aaa authentication username-prompt** command does not change any dialog that is supplied by a remote TACACS+ server.

Examples

The following example changes the text for the username prompt:

```
aaa authentication username-prompt “Enter your name here:”
```

Related Commands

Command	Description
aaa authentication password-prompt	Changes the text that is displayed when users are prompted for a password.
aaa new-model	Enables the AAA access control model.
enable password	Sets a local password to control access to various privilege levels.

aaa authorization

To set the parameters that restrict user access to a network, use the **aaa authorization** command in global configuration mode. To remove the parameters, use the **no** form of this command.

aaa authorization {**auth-proxy** | **cache** | **commands** *level* | **config-commands** | **configuration** | **console** | **exec** | **ipmobile** | **multicast** | **network** | **policy-if** | **prepaid** | **radius-proxy** | **reverse-access** | **subscriber-service** | **template**} {**default** | *list-name*} [*method1* [*method2*...]]

no aaa authorization {**auth-proxy** | **cache** | **commands** *level* | **config-commands** | **configuration** | **console** | **exec** | **ipmobile** | **multicast** | **network** | **policy-if** | **prepaid** | **radius-proxy** | **reverse-access** | **subscriber-service** | **template**} {**default** | *list-name*} [*method1* [*method2*...]]

Syntax Description

auth-proxy	Runs authorization for authentication proxy services.
cache	Configures the authentication, authorization, and accounting (AAA) server.
commands	Runs authorization for all commands at the specified privilege level.
level	Specific command level that should be authorized. Valid entries are 0 through 15.
config-commands	Runs authorization to determine whether commands entered in configuration mode are authorized.
configuration	Downloads the configuration from the AAA server.
console	Enables the console authorization for the AAA server.
exec	Runs authorization to determine if the user is allowed to run an EXEC shell. This facility returns user profile information such as the autocommand information.
ipmobile	Runs authorization for mobile IP services.
multicast	Downloads the multicast configuration from the AAA server.
network	Runs authorization for all network-related service requests, including Serial Line Internet Protocol (SLIP), PPP, PPP Network Control Programs (NCPs), and AppleTalk Remote Access (ARA).
policy-if	Runs authorization for the diameter policy interface application.
prepaid	Runs authorization for diameter prepaid services.
radius-proxy	Runs authorization for proxy services.
reverse-access	Runs authorization for reverse access connections, such as reverse Telnet.
subscriber-service	Runs authorization for iEdge subscriber services such as virtual private dialup network (VPDN).
template	Enables template authorization for the AAA server.
default	Uses the listed authorization methods that follow this keyword as the default list of methods for authorization.
list-name	Character string used to name the list of authorization methods.
method1 [*method2*...]	(Optional) Identifies an authorization method or multiple authorization methods to be used for authorization. A method may be any one of the keywords listed in Table 8.

Command Default

Authorization is disabled for all actions (equivalent to the method keyword **none**).

Command Modes Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	This command was modified. The **group radius** and **group tacacs+** keywords were added as methods for authorization.
12.2(28)SB	This command was modified. The **cache** *group-name* keyword and argument were added as a method for authorization.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.1(1)T	This command was modified. The **group ldap** keyword was added.

Usage Guidelines Use the **aaa authorization** command to enable authorization and to create named methods lists, which define authorization methods that can be used when a user accesses the specified function. Method lists for authorization define the ways in which authorization will be performed and the sequence in which these methods will be performed. A method list is a named list that describes the authorization methods (such as RADIUS or TACACS+) that must be used in sequence. Method lists enable you to designate one or more security protocols to be used for authorization, thus ensuring a backup system in case the initial method fails. Cisco IOS software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS software selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or until all the defined methods are exhausted.

Note The Cisco IOS software attempts authorization with the next listed method only when there is no response from the previous method. If authorization fails at any point in this cycle—meaning that the security server or the local username database responds by denying the user services—the authorization process stops and no other authorization methods are attempted.

If the **aaa authorization** command for a particular authorization type is issued without a specified named method list, the default method list is automatically applied to all interfaces or lines (where this authorization type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no authorization takes place. The default authorization method list must be used to perform outbound authorization, such as authorizing the download of IP pools from the RADIUS server.

Use the **aaa authorization** command to create a list by entering the values for the *list-name* and the *method* arguments, where *list-name* is any character string used to name this list (excluding all method names) and *method* identifies the list of authorization methods tried in the given sequence.

Note In Table 8, the **group** *group-name,* **group ldap, group radius**, and **group tacacs+** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the host servers. Use the **aaa group server radius**, **aaa group server ldap**, and **aaa group server tacacs+** commands to create a named group of servers.

Table 8 describes the method keywords.

Table 8 aaa authorization Methods

Keyword	Description
cache *group-name*	Uses a cache server group for authorization.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the **server group** *group-name* command.
group ldap	Uses the list of all Lightweight Directory Access Protocol (LDAP) servers for authentication.
group radius	Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command.
group tacacs+	Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command.
if-authenticated	Allows the user to access the requested function if the user is authenticated. **Note** The **if-authenticated** method is a terminating method. Therefore, if it is listed as a method, any methods listed after it will never be evaluated.
local	Uses the local database for authorization.
none	Indicates that no authorization is performed.

Cisco IOS software supports the following methods for authorization:

- Cache Server Groups—The router consults its cache server groups to authorize specific rights for users.
- If-Authenticated—The user is allowed to access the requested function provided the user has been authenticated successfully.
- Local—The router or access server consults its local database, as defined by the **username** command, to authorize specific rights for users. Only a limited set of functions can be controlled through the local database.
- None—The network access server does not request authorization information; authorization is not performed over this line or interface.
- RADIUS—The network access server requests authorization information from the RADIUS security server group. RADIUS authorization defines specific rights for users by associating attributes, which are stored in a database on the RADIUS server, with the appropriate user.
- TACACS+—The network access server exchanges authorization information with the TACACS+ security daemon. TACACS+ authorization defines specific rights for users by associating attribute-value (AV) pairs, which are stored in a database on the TACACS+ security server, with the appropriate user.

Method lists are specific to the type of authorization being requested. AAA supports five different types of authorization:

- Commands—Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- EXEC—Applies to the attributes associated with a user EXEC terminal session.

- Network—Applies to network connections. The network connections can include a PPP, SLIP, or ARA connection.

Note You must configure the **aaa authorization config-commands** command to authorize global configuration commands, including EXEC commands prepended by the **do** command.

- Reverse Access—Applies to reverse Telnet sessions.
- Configuration—Applies to the configuration downloaded from the AAA server.

When you create a named method list, you are defining a particular list of authorization methods for the indicated authorization type.

Once defined, the method lists must be applied to specific lines or interfaces before any of the defined methods are performed.

The authorization command causes a request packet containing a series of AV pairs to be sent to the RADIUS or TACACS daemon as part of the authorization process. The daemon can do one of the following:

- Accept the request as is.
- Make changes to the request.
- Refuse the request and authorization.

For a list of supported RADIUS attributes, see the module *RADIUS Attributes*. For a list of supported TACACS+ AV pairs, see the module *TACACS+ Attribute-Value Pairs*.

Note Five commands are associated with privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. If you configure AAA authorization for a privilege level greater than 0, these five commands will not be included in the privilege level command set.

Examples

The following example shows how to define the network authorization method list named mygroup, which specifies that RADIUS authorization will be used on serial lines using PPP. If the RADIUS server fails to respond, local network authorization will be performed.

```
aaa authorization network mygroup group radius local
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
aaa group server tacacs+	Groups different TACACS+ server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.
tacacs-server host	Specifies a TACACS+ host.
username	Establishes a username-based authentication system.

aaa authorization (IKEv2 profile)

To specify AAA authorization for a local or external group policy, use the **aaa authorization** command in IKEv2 profile configuration mode. To remove the AAA authorization, use the **no** form of this command.

aaa authorization {**group** | **user**}{**cert** | **eap** | **psk**}{*aaa-name aaa-username* | **name-mangler** *mangler-name*}

no aaa authorization {**group** | **user**}{**cert** | **eap** | **psk**} *aaa-name*

Syntax Description

group	Specifies AAA authorization for local or external group policy.
user	Specifies AAA authorization for each user policy
cert	Specifies the AAA method list that is used when the remote authentication method is certificate based.
eap	Specifies the AAA method list that is used when the remote authentication method is Extensible Authentication Protocol (EAP).
psk	Specifies the AAA method list that is used when the remote authentication method is preshared key.
aaa-name	The AAA list name.
aaa-username	The AAA username.
name-mangler *mangler-name*	Derives the name mangler from the **crypto ikev2 name-mangler** command.

Command Default

AAA authorization is not specified.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.1(3)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to specify AAA authorization for local or external group policy. The **crypto ikev2 profile** command must be enabled before this command is executed.

Note If no AAA method list is specified, the list is common for all authentication methods. Local AAA is not supported for user authorization.

The following is the order of precedence among group and user policies:

- AAA user policy

- AAA group policy

Note The **user** keyword is not required and not recommended when RADIUS is the external AAA server as RADIUS combines authentication and authorization and returns authorization data with successful authentication. The user keyword can be used with AAA servers such as TACACS+ where authentication and authorization are decoupled.

Examples

The following example shows how to configure the AAA authorization for a local group policy. The aaa-group-list specifies that group authorization is local and the AAA username is abc. The authorization list name corresponds to the group policy defined in the **crypto ikev2 authorization policy** command.

```
Router(config)# aaa new-model
Router(config)# aaa authorization network aaa-group-list default local
Router(config)# crypto ikev2 authorization policy 123
Router(config-ikev2-client-config-group)# pool addr-pool1
Router(config-ikev2-client-config-group)# dns 198.51.100.1 198.51.100.100
Router(config-ikev2-client-config-group)# wins 203.0.113.1 203.0.113.115
Router(config-ikev2-client-config-group)# exit
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# wins 203.0.113.1 203.0.113.115 authentication remote eap
Router(config-ikev2-profile)# aaa authorization group aaa-group-list abc
```

The following example shows how to configure an external AAA-based group policy. The aaa-group-list specifies that the group authorization is RADIUS based. The name mangler derives the group name from the domain part of ID-FQDN, which is abc.'

```
Router(config)# aaa new-model
Router(config)# aaa authorization network aaa-group-list default group radius
Router(config)# crypto ikev2 name-mangler mangler1
Router(config-ikev2-name-mangler)# fqdn domain
Router(config-ikev2-name-mangler)# exit
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# identity remote fqdn host1.abc
Router(config-ikev2-profile)# authentication remote eap
Router(config-ikev2-profile)# aaa authorization group aaa-group-list name-mangler mangler1
```

The following example shows how to configure an external AAA-based group policy. The aaa-user-list specifies that user authorization is RADIUS based. The name mangler derives the username from hostname part of ID-FQDN, which is host1.

```
Router(config)# aaa new-model
Router(config)# aaa authorization network aaa-user-list default group radius
Router(config)# crypto ikev2 name-mangler mangler2
Router(config-ikev2-name-mangler)# fqdn hostname
Router(config-ikev2-name-mangler)# exit
Router(config-ikev2-profile)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# match identity remote fqdn host1.abc
Router(config-ikev2-profile)# authentication remote eap
Router(config-ikev2-profile)# aaa authorization user aaa-user-list name-mangler mangler2
```

Related Commands

Command	Description
crypto ikev2 name-mangler	Defines a name mangler.
crypto ikev2 profile	Defines an IKEv2 profile.

aaa authorization cache filterserver

To enable authentication, authorization, and accounting (AAA) authorization caches and the downloading of access control list (ACL) configurations from a RADIUS filter server, use the **aaa authorization cache filterserver** command in global configuration mode. To disable AAA authorization caches, use the **no** form of this command.

aaa authorization cache filterserver default *methodlist* [*methodlist2...*]

no aaa authorization cache filterserver default

Syntax Description

default	Default authorization list.
methodlist [*methodlist2...*]	One of the keywords listed in Table 9.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Use the **aaa authorization cache filterserver** command to enable the RADIUS ACL filter server.

Method keywords are described in Table 9.

Table 9 aaa authorization cache filterserver Methods

Keyword	Description
group *group-name*	Uses a subset of RADIUS servers for authentication as defined by the **aaa group server radius** command.
local	Uses the local database for authorization caches and ACL configuration downloading.
none	No authorization is performed.

This command functions similarly to the **aaa authorization** command with the following exceptions:

- Named method-lists cannot be configured.
- Only one instance of this command can be configured.
- TACACS+ groups cannot be configured.

Examples

The following example shows how to configure the default RADIUS server group as the desired filter. If the request is rejected or a reply is not returned, local configuration will be consulted. If the local filter does not respond, the call will be accepted but filtering will not occur.

```
aaa authorization cache filterserver group radius local none
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.

aaa authorization config-commands

To reestablish the default created when the **aaa authorization commands** command was issued, use the **aaa authorization config-commands** command in global configuration mode. To disable authentication, authorization, and accounting (AAA) configuration command authorization, use the **no** form of this command.

aaa authorization config-commands

no aaa authorization config-commands

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.0(6.02)T	This command was changed from being enabled by default to being disabled by default.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the **aaa authorization commands** *level method* command is enabled, all commands, including configuration commands, are authorized by authentication, authorization, and accounting (AAA) using the method specified. Because there are configuration commands that are identical to some EXEC-level commands, there can be some confusion in the authorization process. Using the **no aaa authorization config-commands** command stops the network access server from attempting configuration command authorization.

After the **no** form of this command has been entered, AAA authorization of configuration commands is completely disabled. Care should be taken before entering the **no** form of this command because it potentially reduces the amount of administrative control on configuration commands.

Use the **aaa authorization config-commands** command if, after using the **no** form of this command, you need to reestablish the default set by the **aaa authorization commands** *level method* command.

Note You will get the same result if you (1) do not configure this command, or (2) configure **no aaa authorization config-commands**.

Examples

The following example specifies that TACACS+ authorization is run for level 15 commands and that AAA authorization of configuration commands is disabled:

```
aaa new-model
aaa authorization command 15 group tacacs+ none
no aaa authorization config-commands
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.

aaa authorization console

To apply authorization to a console, use the **aaa authorization console** command in global configuration mode. To disable the authorization, use the **no** form of this command.

aaa authorization console

no aaa authorization console

Syntax Description

This command has no arguments or keywords.

Defaults

Authentication, authorization, and accounting (AAA) authorization is disabled on the console.

Command Modes

Global configuration

Command History

Release	Modification
12.0(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the **aaa new-model** command has been configured to enable the AAA access control model, the **no aaa authorization console** command is the default, and the authorization that is configured on the console line will always succeed. If you do not want the default, you need to configure the **aaa authorization console** command.

Note This command by itself does not turn on authorization of the console line. It needs to be used in conjunction with the **authorization** command under console line configurations.

If you are trying to enable authorization and the **no aaa authorization console** command is configured by default, you will see the following message:

```
%Authorization without the global command aaa authorization console is useless.
```

Examples

The following example shows that the default authorization that is configured on the console line is being disabled:

```
Router (config)# aaa authorization console
```

Related Commands

Command	Description
authorization	Enables AAA authorization for a specific line or group of lines.

aaa authorization list

To allow user attributes to get "pushed" during authentication, use the **aaa authorization list** command in webvpn context configuration mode. To disable the pushing of attributes, use the **no** form of this command.

aaa authorization list

no aaa authorization list

Syntax Description

name	Name of the list to be automatically authorized.

Command Default

User attributes are not pushed during authentication.

Command Modes

Webvpn context (config-webvpn-context)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

If this command is configured, a separate authorization step is no longer needed after authentication.

Examples

The following example shows that authorization is to be pushed during authentication for List 11:

```
Router (config)# webvpn context
Router (config-webvpn-context)# aaa authorization list 11
```

Related Commands

Command	Description
aaa authentication auto (WebVPN)	Allows automatic authentication for SSL VPN users.

aaa authorization reverse-access

To configure a network access server to request authorization information from a security server before allowing a user to establish a reverse Telnet session, use the **aaa authorization reverse-access** command in global configuration mode. To restore the default value for this command, use the **no** form of this command.

aaa authorization reverse-access {**group radius** | **group tacacs+**}

no aaa authorization reverse-access {**group radius** | **group tacacs+**}

Syntax Description

group radius	Specifies that the network access server will request authorization from a RADIUS security server before allowing a user to establish a reverse Telnet session.
group tacacs+	Specifies that the network access server will request authorization from a TACACS+ security server before allowing a user to establish a reverse Telnet session.

Defaults

This command is disabled by default, meaning that authorization for reverse Telnet is not requested.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(5)T	Group server support was added as various method keywords for this command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Telnet is a standard terminal emulation protocol used for remote terminal connection. Normally, you log in to a network access server (typically through a dialup connection) and then use Telnet to access other network devices from that network access server. There are times, however, when it is necessary to establish a reverse Telnet session. In reverse Telnet sessions, the Telnet connection is established in the opposite direction—from inside a network to a network access server on the network periphery to gain access to modems or other devices connected to that network access server. Reverse Telnet is used to provide users with dialout capability by allowing them to open Telnet sessions to modem ports attached to a network access server.

It is important to control access to ports accessible through reverse Telnet. Failure to do so could, for example, allow unauthorized users free access to modems where they can trap and divert incoming calls or make outgoing calls to unauthorized destinations.

Authentication during reverse Telnet is performed through the standard AAA login procedure for Telnet. Typically the user has to provide a username and password to establish either a Telnet or reverse Telnet session. This command provides an additional (optional) level of security by requiring authorization in

addition to authentication. When this command is enabled, reverse Telnet authorization can use RADIUS or TACACS+ to authorize whether or not this user is allowed reverse Telnet access to specific asynchronous ports, after the user successfully authenticates through the standard Telnet login procedure.

Examples

The following example causes the network access server to request authorization information from a TACACS+ security server before allowing a user to establish a reverse Telnet session:

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization reverse-access default group tacacs+
!
tacacs-server host 172.31.255.0
tacacs-server timeout 90
tacacs-server key goaway
```

The lines in this sample TACACS+ reverse Telnet authorization configuration are defined as follows:

- The **aaa new-model** command enables AAA.
- The **aaa authentication login default group tacacs+** command specifies TACACS+ as the default method for user authentication during login.
- The **aaa authorization reverse-access default group tacacs+** command specifies TACACS+ as the method for user authorization when trying to establish a reverse Telnet session.
- The **tacacs-server host** command identifies the TACACS+ server.
- The **tacacs-server timeout** command sets the interval of time that the network access server waits for the TACACS+ server to reply.
- The **tacacs-server key** command defines the encryption key used for all TACACS+ communications between the network access server and the TACACS+ daemon.

The following example configures a generic TACACS+ server to grant a user, “jim,” reverse Telnet access to port tty2 on the network access server named “site1” and to port tty5 on the network access server named site2:

```
user = jim
  login = cleartext lab
  service = raccess {
    port#1 = site1/tty2
    port#2 = site2/tty5
}
```

Note In this example, “site1” and “site2” are the configured host names of network access servers, not DNS names or alias.

The following example configures the TACACS+ server (CiscoSecure) to authorize a user named Jim for reverse Telnet:

```
user = jim
 profile_id = 90
 profile_cycle = 1
 member = Tacacs_Users
 service=shell {
 default cmd=permit
 }
 service=raccess {
 allow "c2511e0" "tty1" ".*"
 refuse ".*" ".*" ".*"
```

```
password = clear "goaway"
```

Note CiscoSecure only supports reverse Telnet using the command line interface in versions 2.1(*x*) through version 2.2(1).

An empty "service=raccess {}" clause permits a user to have unconditional access to network access server ports for reverse Telnet. If no "service=raccess" clause exists, the user is denied access to any port for reverse Telnet.

For more information about configuring TACACS+, refer to the chapter "Configuring TACACS+" in the *Cisco IOS Security Configuration Guide*. For more information about configuring CiscoSecure, refer to the *CiscoSecure Access Control Server User Guide*, version 2.1(2) or later.

The following example causes the network access server to request authorization from a RADIUS security server before allowing a user to establish a reverse Telnet session:

```
aaa new-model
aaa authentication login default group radius
aaa authorization reverse-access default group radius
!
radius-server host 172.31.255.0
radius-server key goaway
```

The lines in this sample RADIUS reverse Telnet authorization configuration are defined as follows:

- The **aaa new-model** command enables AAA.
- The **aaa authentication login default group radius** command specifies RADIUS as the default method for user authentication during login.
- The **aaa authorization reverse-access default group radius** command specifies RADIUS as the method for user authorization when trying to establish a reverse Telnet session.
- The **radius-server host** command identifies the RADIUS server.
- The **radius-server key** command defines the encryption key used for all RADIUS communications between the network access server and the RADIUS daemon.

The following example configures the RADIUS server to grant a user named "jim" reverse Telnet access at port tty2 on network access server site1:

```
Password = "goaway"
User-Service-Type = Shell-User
cisco-avpair = "raccess:port#1=site1/tty2"
```

The syntax "raccess:port=any/any" permits a user to have unconditional access to network access server ports for reverse Telnet. If no "raccess:port={*nasname*}/{*tty number*}" clause exists in the user profile, the user is denied access to reverse Telnet on all ports.

For more information about configuring RADIUS, refer to the chapter "Configuring RADIUS" in the *Cisco IOS Security Configuration Guide*.

aaa authorization template

To enable usage of a local or remote customer template on the basis of Virtual Private Network (VPN) routing and forwarding (VRF), use the **aaa authorization template** command in global configuration mode. To disable the new authorization, use the **no** form of this command.

aaa authorization template

no aaa authorization template

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Examples

The following example enables usage of a remote customer template:

```
aaa authorization template
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.
tacacs-server host	Specifies a TACACS+ server host.
template	Accesses the template configuration mode for configuring a particular customer profile template.

aaa cache filter

To enable filter cache configuration, use the **aaa cache filter** command in global configuration mode. To disable this functionality, use the **no** form of this command.

aaa cache filter

no aaa cache filter

Syntax Description

This command has no arguments or keywords.

Defaults

Filter cache configuration is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Use the **aaa cache filter** command to begin filter cache configuration and enter AAA filter configuration mode (config-aaa-filter).

After enabling this command, you can specify filter cache parameters with the following commands:

- **cache clear age**—Specifies, in minutes, when cache entries expire and the cache is cleared.
- **cache disable**—Disables the cache.
- **cache max**—Refreshes a cache entry when a new sessions begins.
- **cache refresh**—Limits the absolute number of entries the cache can maintain for a particular server.
- **password**—Specifies the optional password that is to be used for filter server authentication requests.

Note Each of these commands is optional; thus, the default value will be enabled for any command that is not specified.

Examples

The following example shows how to enable filter cache configuration and specify cache parameters.

```
aaa cache filter
 password mycisco
 no cache refresh
 cache max 100
```

Related Commands

Command	Description
aaa authorization cache filterserver	Enables AAA authorization caches and the downloading of ACL configurations from a RADIUS filter server.
cache clear age	Specifies when, in minutes, cache entries expire and the cache is cleared.
cache disable	Disables the cache.
cache max	Refreshes a cache entry when a new sessions begins.
cache refresh	Limits the absolute number of entries the cache can maintain for a particular server.
password	Specifies the optional password that is to be used for filter server authentication requests.

aaa cache filterserver

To enable Authentication, Authorization, and Accounting (AAA) filter server definitions, use the **aaa cache filterserver** command in global configuration mode. To disable AAA filter server definitions, use the **no** form of this command.

aaa cache filterserver

no aaa cache filterserver

Syntax Description

This command has no arguments or keywords.

Command Default

This command is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Usage Guidelines

The **aaa cache filterserver** command is mainly used to define AAA cache filter server requirements for downloading access control lists (ACLs) commands but is also used for cache configurations, domain names, and passwords. To use this command, enable the **aaa authorization cache filterserver** command first.

Examples

The following example enables the **aaa cache filterserver** command:

```
Router> enable

Router# configure terminal

Router(config)# aaa new-model

Router (config)# aaa authorization cache filterserver default group radius

Router(config)# aaa cache filterserver

Router(config-filter)# cache max 100

Router(config-filter)# no cache refresh
```

Related Commands

Command	Description
show aaa cache filterserver	Displays the aaa cache filterserver status.

aaa cache profile

To create a named authentication and authorization cache profile group and enter profile map configuration mode, use the **aaa cache profile** command in global configuration mode. To disable a cache profile group, use the **no** form of this command.

aaa cache profile *group-name*

no aaa cache profile *group-name*

Syntax Description

group-name	Text string that specifies an authentication and authorization group. Group names cannot be duplicated.

Command Default

No cache profile groups are defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use this command to define or modify an authentication or authorization cache group and to specify cache profile parameters using the following commands:

- **all**—Specifies that all authentication and authorization requests are cached. Using the **all** command makes sense for certain service authorization requests, but it should be avoided when dealing with authentication requests.
- **profile**—Specifies an exact profile match to cache. The profile name must be an exact match to the username being queried by the service authentication or authorization request. This is the recommended format to enter profiles that users want to cache.
- **regexp**—Allows entries to match based on regular expressions. Matching on regular expressions is not recommended for most situations.

  The **any** keyword, which is available under the **regexp** submenu, allows any unique instance of a AAA server response that matches the regular expression to be saved in the cache. The **only** keyword allows for only one instance of a AAA server response that matches the regular expression to be saved in the cache.

Entering the **no** form of this command deletes the profile definition and all of its command definitions.

Examples

The following example creates the AAA cache profile group localusers:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa cache profile localusers
```

Related Commands

Command	Description
all	Specifies that all authentication and authorization requests be cached.
profile	Defines or modifies an individual authentication and authorization cache profile.
regexp	Creates an entry in a cache profile group that allows authentication and authorization matches based on a regular expression.

aaa configuration

To configure the username and password that are to be used when downloading configuration requests, an IP pool, or static routes through RADIUS, use the **aaa configuration** command in global configuration mode. To disable this feature, use the **no** form of this command.

aaa configuration {**config-username** | **pool** | **route**} **username** *username* [**password** [**0** | **7**] *password*]

no aaa configuration {**config-username** | **pool** | **route**} **username** *username* [**password** [**0** | **7**] *password*]

Syntax Description

config-username	Configures the username and password used in configuration requests that can be downloaded.
pool	Configures the username and password used for downloading an IP pool. IP pools are used to define range of IP addresses that are used for Dynamic Host Configuration Protocol (DHCP) servers and point-to-point servers.
route	Configures the username and password used when downloading static routes through RADIUS.
username *username*	Defines a username to be used instead of the router's hostname.
password *password*	(Optional) Defines an alphanumeric password to be used instead of the default "cisco."
0 | **7**	(Optional) Defines whether the text immediately following is encrypted, and, if so, what type of encryption is used. • **0**—The text immediately following is not encrypted. **Note** Type 0 passwords are automatically converted to type 7 passwords by enabling the **service password-encryption** command. • **7**—The text is encrypted using a Cisco-defined encryption algorithm .

Defaults

The hostname of the router and the password "cisco" are used during the static route configuration download.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

The **aaa configuration** command allows you to specify a username other than the router's hostname and a stronger password than the default "cisco."

Examples

The following example shows how to specify the username “MyUsername” and the password “MyPass” when downloading a static route configuration:

```
aaa new-model
aaa group server radius rad1
    server 10.1.1.1
    exit
aaa authorization configuration default group radius
aaa authorization configuration foo group rad1
aaa route download 1 authorization foo
aaa configuration route username MyUsername password 0 MyPass
radius-server host 10.2.2.2
radius-server key 0 RadKey
```

Related Commands

Command	Description
aaa route download	Enables the static route download feature and sets the amount of time between downloads.
service password-encryption	Enables 0 (non-encrypted) passwords to be automatically converted to type 7 (encrypted) passwords.

aaa dnis map accounting network

To map a Dialed Number Information Service (DNIS) number to a particular authentication, authorization, and accounting (AAA) server group that will be used for AAA accounting, use the **aaa dnis map accounting network** command in global configuration mode. To remove DNIS mapping from the named server group, use the **no** form of this command.

aaa dnis map *dnis-number* **accounting network** [**start-stop** | **stop-only** | **none**] [**broadcast**] **group** *groupname*

no aaa dnis map *dnis-number* **accounting network**

Syntax Description

dnis-number	Number of the DNIS.
start-stop	(Optional) Indicates that the defined security server group will send a "start accounting" notice at the beginning of a process and a "stop accounting" notice at the end of a process. The "start accounting" record is sent in the background. (The requested user process begins regardless of whether the "start accounting" notice was received by the accounting server.)
stop-only	(Optional) Indicates that the defined security server group will send a "stop accounting" notice at the end of the requested user process.
none	(Optional) Indicates that the defined security server group will not send accounting notices.
broadcast	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.
group *groupname*	At least one of the keywords described in Table 10.

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1(1)T	• The optional **broadcast** keyword was added. • The ability to specify multiple server groups was added. • To accommodate multiple server groups, the name of the command was changed from **aaa dnis map accounting network group** to **aaa dnis map accounting network**.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command lets you assign a DNIS number to a particular AAA server group so that the server group can process accounting requests for users dialing in to the network using that particular DNIS. To use this command, you must first enable AAA, define an AAA server group, and enable DNIS mapping.

Table 10 contains descriptions of accounting method keywords.

Table 10 AAA Accounting Methods

Keyword	Description
group radius	Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius command.**
group tacacs+	Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group *group-name*.

In Table 10, the **group radius** and **group tacacs+** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs+-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Examples

The following example maps DNIS number 7777 to the RADIUS server group called group1. Server group group1 will use RADIUS server 172.30.0.0 for accounting requests for users dialing in with DNIS 7777.

```
aaa new-model
radius-server host 172.30.0.0 acct-port 1646 key cisco1
aaa group server radius group1
 server 172.30.0.0
aaa dnis map enable
aaa dnis map 7777 accounting network group group1
```

Related Commands

Command	Description
aaa dnis map authentication ppp group	Maps a DNIS number to a particular authentication server group.
aaa dnis map enable	Enables AAA server selection based on DNIS.
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.

aaa dnis map authentication group

To map a dialed number identification service (DNIS) number to a particular authentication server group (this server group will be used for authentication, authorization, and accounting [AAA] authentication), use the **aaa dnis map authentication group** command in AAA-server-group configuration mode. To remove the DNIS number from the defined server group, use the **no** form of this command.

aaa dnis map *dnis-number* **authentication** {**ppp** | **login**} **group** *server-group-name*

no aaa dnis map *dnis-number* **authentication** {**ppp** | **login**} **group** *server-group-name*

Syntax Description

dnis-number	Number of the DNIS.
ppp	Enables PPP authentication methods.
login	Enables character-mode authentication.
server-group-name	Character string used to name a group of security servers associated in a server group.

Command Default

A DNIS number is not mapped to a server group.

Command Modes

AAA-server-group configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1(3)XL1	This command was modified with the addition of the **login** keyword to include character-mode authentication.
12.2(2)T	Support for the **login** keyword was added into Cisco IOS Release 12.2(2)T and this command was implemented for the Cisco 2600 series, Cisco 3600 series, and Cisco 7200 platforms.
12.2(8)T	This command was implemented on the Cisco 806, Cisco 828, Cisco 1710, Cisco SOHO 78, Cisco 3631, Cisco 3725, Cisco 3745, and Cisco URM for IGX8400 platforms.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5800 platforms.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **aaa dnis map authentication group** command to assign a DNIS number to a particular AAA server group so that the server group can process authentication requests for users that are dialing in to the network using that particular DNIS. To use the **aaa dnis map authentication group** command, you must first enable AAA, define a AAA server group, and enable DNIS mapping.

Examples

The following example maps DNIS number 7777 to the RADIUS server group called group1. Server group group1 uses RADIUS server 172.30.0.0 for authentication requests for users dialing in with DNIS number 7777.

```
aaa new-model
radius-server host 172.30.0.0 auth-port 1645 key cisco1
aaa group server radius group1
 server 172.30.0.0
 aaa dnis map enable
 aaa dnis map 7777 authentication ppp group group1
 aaa dnis map 7777 authentication login group group1
```

Related Commands

Command	Description
aaa dnis map accounting network group	Maps a DNIS number to a particular accounting server group.
aaa dnis map enable	Enables AAA server selection based on DNIS.
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.

aaa dnis map authorization network group

To map a Dialed Number Identification Service (DNIS) number to a particular authentication, authorization, and accounting (AAA) server group (the server group that will be used for AAA authorization), use the **aaa dnis map authorization network group** command in global configuration mode. To unmap this DNIS number from the defined server group, use the **no** form of this command.

aaa dnis map *dnis-number* **authorization network group** *server-group-name*

no aaa dnis map *dnis-number* **authorization network group** *server-group-name*

Syntax Description

dnis-number	Number of the DNIS.
server-group-name	Character string used to name a group of security servers functioning within a server group.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command lets you assign a DNIS number to a particular AAA server group so that the server group can process authorization requests for users dialing in to the network using that particular DNIS number. To use this command, you must first enable AAA, define a AAA server group, and enable DNIS mapping.

Examples

The following example maps DNIS number 7777 to the RADIUS server group called group1. Server group group1 will use RADIUS server 172.30.0.0 for authorization requests for users dialing in with DNIS 7777:

```
aaa new-model
radius-server host 172.30.0.0 auth-port 1645 key cisco1
aaa group server radius group1
server 172.30.0.0
aaa dnis map enable
aaa dnis map 7777 authorization network group group1
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
aaa dnis map accounting network group	Maps a DNIS number to a AAA server group used for accounting services.
aaa dnis map authentication ppp group	Maps a DNIS number to a AAA server used for authentication services.
aaa dnis map enable	Enables AAA server selection based on DNIS number.
aaa group server	Groups different server hosts into distinct lists and methods.
radius-server host	Specifies and defines the IP address of the RADIUS server host.

aaa group server diameter

To group different Diameter server hosts into distinct lists and distinct methods, enter the **aaa group server diameter** command in global configuration mode. To remove a group server from the configuration list, enter the **no** form of this command.

aaa group server diameter *group-name*

no aaa group server diameter *group-name*

Syntax Description

group-name	Character string used to name the group of servers.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

The **aaa group server diameter command** introduces a way to group existing server hosts. This command enables you to select a subset of the configured server hosts and use them for a particular service.

A group server is a list of server hosts of a particular type. Currently supported server host types are Diameter server hosts, RADIUS server hosts, and TACACS+ server hosts. A group server is used in conjunction with a global server host list. The group server lists the IP addresses of the selected server hosts.

Examples

The following example shows the configuration of a Diameter server group named dia_group_1 that comprises two member servers configured as Diameter peers:

```
aaa group server diameter dia_group_1
 server dia_peer_1
 server dia_peer_2
```

Note If a peer port is not specified, the default value for the peer port is 3868.

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication login	Sets AAA authentication at login.

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.
server	Associates a Diameter server with a Diameter server group.

aaa group server ldap

To group different Lightweight Directory Access Protocol (LDAP) servers into distinct lists and distinct methods, use the **aaa group server ldap** command in global configuration mode. To remove a group server from the configuration list, enter the **no** form of this command.

aaa group server ldap *group-name*

no aaa group server ldap *group-name*

Syntax Description

group-name	Name of the server groups.

Command Default

No LDAP servers are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

The **aaa group server ldap** command enables you to group existing servers. This command allows you to select a subset of the configured server and use them for a particular service.

A group server is a list of servers of a particular type. A group server is used in conjunction with a global server host list. The group server lists the IP addresses of the selected server hosts.

Examples

The following example shows how to configure an LDAP server group named ldp_group_1:

```
Router> enable
Router(config)# aaa group server ldp_group_1
```

Related Commands

Command	Description
aaa authentication login	Sets AAA authentication at login.
aaa authorization	Sets parameters that restrict user access to a network.
ldap server	Defines an LDAP server and enters LDAP server configuration mode.

aaa group server radius

To group different RADIUS server hosts into distinct lists and distinct methods, enter the **aaa group server radius** command in global configuration mode. To remove a group server from the configuration list, enter the **no** form of this command.

aaa group server radius *group-name*

no aaa group server radius *group-name*

Syntax Description

group-name	Character string used to name the group of servers. See Table 11 for a list of words that cannot be used as the *group-name* argument.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The authentication, authorization, and accounting (AAA) server-group feature introduces a way to group existing server hosts. The feature enables you to select a subset of the configured server hosts and use them for a particular service.

A group server is a list of server hosts of a particular type. Currently supported server host types are RADIUS server hosts and TACACS+ server hosts. A group server is used in conjunction with a global server host list. The group server lists the IP addresses of the selected server hosts.

Table 11 lists words that cannot be used as the *group-name* argument.

Table 11 Words That Cannot Be Used As the group-name Argument

Word
auth-guest
enable
guest
if-authenticated
if-needed

Table 11 Words That Cannot Be Used As the group-name Argument (continued)

Word
krb5
krb-instance
krb-telnet
line
local
none
radius
rcmd
tacacs
tacacsplus

Examples

The following example shows the configuration of an AAA group server named radgroup1 that comprises three member servers:

```
aaa group server radius radgroup1
 server 10.1.1.1 auth-port 1700 acct-port 1701
 server 10.2.2.2 auth-port 1702 acct-port 1703
 server 10.3.3.3 auth-port 1705 acct-port 1706
```

Note If auth-port and acct-port are not specified, the default value of auth-port is 1645 and the default value of acct-port is 1646.

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication login	Set AAA authentication at login.
aaa authorization	Sets parameters that restrict user access to a network.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.

aaa group server tacacs+

To group different TACACS+ server hosts into distinct lists and distinct methods, use the **aaa group server tacacs+** command in global configuration mode. To remove a server group from the configuration list, use the **no** form of this command.

aaa group server tacacs+ *group-name*

no aaa group server tacacs+ *group-name*

Syntax Description

group-name	Character string used to name the group of servers. See Table 12 for a list of words that cannot be used as the *group-name* argument.

Defaults

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(54)SG	This command was integrated into Cisco IOS Release 12.2(54)SG.

Usage Guidelines

The authentication, authorization, and accounting (AAA) server-group feature introduces a way to group existing server hosts. The feature enables you to select a subset of the configured server hosts and use them for a particular service.

A server group is a list of server hosts of a particular type. Currently supported server host types are RADIUS server hosts and TACACS+ server hosts. A server group is used in conjunction with a global server host list. The server group lists the IP addresses of the selected server hosts.

Table 12 lists words that cannot be used as the *group-name* argument.

Table 12 Words That Cannot Be Used As the group-name Argument

Word
auth-guest
enable
guest
if-authenticated

Table 12 Words That Cannot Be Used As the group-name Argument (continued)

Word
if-needed
krb5
krb-instance
krb-telnet
line
local
none
radius
rcmd
tacacs
tacacsplus

The following example shows the configuration of an AAA group server named tacgroup1 that comprises three member servers:

```
aaa group server tacacs+ tacgroup1
    server 10.1.1.1
    server 10.2.2.2
    server 10.3.3.3
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security.
aaa authentication login	Enables AAA accounting of requested services for billing or security purposes.
aaa authorization	Sets parameters that restrict user access to a network.
aaa new-model	Enables the AAA access control model.
tacacs-server host	Specifies a TACACS+ host.

aaa intercept

To enable lawful intercept on a router, use the **aaa intercept** command in global configuration mode. To disable lawful intercept, use the **no** form of this command.

aaa intercept

no aaa intercept

Syntax Description

This command has no arguments or keywords.

Command Default

Lawful intercept is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into CiscoIOS XE Release 2.6.

Usage Guidelines

Use the **aaa intercept** command to enable a RADIUS-Based Lawful Intercept solution on your router. Intercept requests are sent (via Access-Accept packets or CoA-Request packets) to the network access server (NAS) or the Layer 2 Tunnel Protocol (L2TP) access concentrator (LAC) from the RADIUS server. All data traffic going to or from a PPP or L2TP session is passed to a mediation device.

Configure this command with high administrative security so that unauthoried people cannot remove the command.

Examples

The following example shows the configuration of a RADIUS-Based Lawful Intercept solution on a router acting as NAS device employing a PPP over Ethernet (PPPoEo) link:

```
aaa new-model
!
aaa intercept
!
aaa group server radius SG
server 10.0.56.17 auth-port 1645 acct-port 1646
!
aaa authentication login LOGIN group SG
aaa authentication ppp default group SG
aaa authorization network default group SG
aaa accounting send stop-record authentication failure
aaa accounting network default start-stop group SG
!
aaa server radius dynamic-author
client 10.0.56.17 server-key cisco
!
```

```
vpdn enable
!
bba-group pppoe PPPoE-TERMINATE
virtual-template 1
!
interface Loopback0
ip address 10.1.1.2 255.255.255.0
!
interface FastEthernet4/1/0
description To RADIUS server
ip address 10.0.56.20 255.255.255.0
duplex auto
!
interface FastEthernet4/1/2
description To network
ip address 10.1.1.1 255.255.255.0
duplex auto
!
interface FastEthernet5/0/0
description To subscriber
no ip address
!
interface FastEthernet5/0/0.1 point-to-point
pvc 10/808
protocol pppoe group PPPoE-TERMINATE
!
interface Virtual-Template1
ip unnumbered Loopback0
ppp authentication chap
!
radius-server attribute 44 include-in-access-req
radius-server attribute nas-port format d
radius-server host 10.0.56.17 auth-port 1645 acct-port 1646
radius-server key cisco
```

aaa local authentication attempts max-fail

To specify the maximum number of unsuccessful authentication attempts before a user is locked out, use the **aaa local authentication attempts max-fail** command in global configuration mode. To remove the setting for the number of unsuccessful attempts, use the **no** form of this command.

aaa local authentication attempts max-fail *number-of-unsuccessful-attempts*

no aaa local authentication attempts max-fail *number-of-unsuccessful-attempts*

Syntax Description

number-of-unsuccessful-attempts	Number of unsuccessful authentication attempts.

Defaults

The Login Password Retry Lockout feature is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

A system message is generated when a user is either locked by the system or unlocked by the system administrator:

```
%AAA-5-USER_LOCKED: User user1 locked out on authentication failure.
```

An administrator cannot be locked out.

Note No messages are displayed to users after authentication failures that are due to the locked status (that is, there is no distinction between a normal authentication failure and an authentication failure due to the locked status of the user).

Note Unconfiguring this command will maintain the status of the user with respect to locked-out or number-of-failed attempts. To clear the existing locked-out or number-of-failed attempts, the system administrator has to explicitly clear the status of the user using **clear** commands.

Examples

The following example illustrates that the maximum number of unsuccessful authentication attempts before a user is locked out has been set for 2:

```
username sysadmin
username sysad privilege 15 password 0 cisco
username user1 password 0 cisco
```

```
aaa new-model
aaa local authentication attempts max-fail 2
!
!
aaa authentication login default local
aaa dnis map enable
aaa session-id common
ip subnet-zero
```

Related Commands

Command	Description
clear aaa local user fail-attempts	Clears the unsuccessful login attempts of the user.
clear aaa local user lockout	Unlocks the locked-out user.
show aaa local user locked	Displays a list of all locked-out users.

aaa max-sessions

To set the maximum number of simultaneous authentication, authorization, and accounting (AAA) connections permitted for a user, use the **aaa max-sessions** command in global configuration mode. To disable the maximum number of sessions, use the **no** form of this command.

aaa max-sessions *maximum-number-of-sessions*

no aaa max-sessions

Syntax Description

maximum-number-of-sessions	Number of estimated AAA maximum sessions. The range is from 1024 to 64000.

Command Default

The default value for **aaa max-sessions** command is platform dependent.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The **aaa max-sessions** command enables you to set the maximum number of simultaneous connections permitted for a user. The **aaa max-sessions** command can be used only if the **aaa new-model** command is configured.

Examples

The following example shows how to adjust the initial hash size for the maximum number of simultaneous AAA sessions:

```
Router# configure terminal
Router(config)# aaa max-sessions 1025
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.

aaa memory threshold

To set appropriate threshold values for the authentication, authorization, and accounting (AAA) memory parameters, use the **aaa memory threshold** command in global configuration mode. To remove threshold values for the AAA memory parameters, use the **no** form of this command.

aaa memory threshold {**accounting disable** *available-memory* | **authentication reject** *available-memory*}

no aaa memory threshold {**accounting disable | authentication reject**}

Syntax Description

accounting	Sets the AAA accounting low-memory threshold.
disable	Disables the accounting threshold, if the available memory falls below the specified percentage.
available-memory	Available memory threshold. The range is from 1 to 15.
authentication	Sets the AAA authentication low-memory threshold.
reject	Rejects the AAA authentication request, if the available memory falls below the specified percentage.
available-memory	Available memory threshold. The range is from 2 to 15.

Command Default

The default memory threshold value for authentication is 3, and the default memory threshold value for accounting is 2.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

You must use the **aaa new-model** command to enable AAA.

Examples

The following example shows how to set the threshold values for the AAA accounting low-memory threshold:

```
Router> enable
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa memory threshold accounting disable 2
```

Related Commands

Command	Description
show aaa memory	Displays the output of the AAA data structure memory tracing information.

aaa nas cisco-nas-port use-async-info

To display physical interface information and parent interface details as part of the of the cisco-nas-port vendor-specific attribute (VSA) for login calls, use the **aaa nas cisco-nas-port use-async-info** command in global configuration mode. To disable the command, use the **no** form of the command.

aaa nas cisco-nas-port use-async-info

no aaa nas cisco-nas-port use-async-info

Syntax Description

This command has no arguments or keywords.

Defaults

The cisco-nas-port attribute has the format of tty*x*/*y* for login calls. Physical interface information is not included.

Command Modes

Global configuration

Command History

Release	Modification
12.3(17)	This command was introduced on the Cisco AS5800.

Usage Guidelines

This command enables the display of interface and parent interface details for login calls.

When this command is not configured, the cisco-nas-port attribute provides only tty*x*/*y* information for login calls. No physical interface information is included. For example:

```
Oct 14 18:42:53.113: RADIUS:  Vendor, Cisco       [26]  17
Oct 14 18:42:53.113: RADIUS:   cisco-nas-port     [2]   11  "tty1/2/07"
```

Other calls, such as PPP, include the physical interface and parent interface details. For example:

```
Oct 14 18:36:00.692: RADIUS:  Vendor, Cisco       [26]  33
Oct 14 18:36:00.692: RADIUS:   cisco-nas-port     [2]   27  "Async1/2/07*Serial1/1/2:0"
```

When you issue the **aaa nas cisco-nas-port use-async-info** command, the interface and parent interface details are included in the login calls.

Examples

The following example shows how to enable the display of interface and parent interface details in the login calls:

```
aaa nas cisco-nas-port use-async-info
```

Related Commands

Command	Description
aaa nas port extended	Replaces the NAS-port attribute with RADIUS IETF attribute 26 and displays extended field information.

aaa nas port extended

To replace the NAS-Port attribute with RADIUS IETF attribute 26 and to display extended field information, use the **aaa nas port extended** command in global configuration mode. To display no extended field information, use the **no** form of this command.

aaa nas port extended

no aaa nas port extended

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

On platforms with multiple interfaces (ports) per slot, the Cisco RADIUS implementation will not provide a unique NAS-Port attribute that permits distinguishing between the interfaces. For example, if a dual PRI interface is in slot 1, calls on both Serial1/0:1 and Serial1/1:1 will appear as NAS-Port = 20101 due to the 16-bit field size limitation associated with RADIUS IETF NAS-Port attribute.

In this case, the solution is to replace the NAS-Port attribute with a vendor-specific attribute (RADIUS IETF Attribute 26). Cisco's vendor ID is 9, and the Cisco-NAS-Port attribute is subtype 2. Vendor-specific attributes (VSAs) can be turned on by entering the **radius-server vsa send** command. The port information in this attribute is provided and configured using the **aaa nas port extended** command.

The standard NAS-Port attribute (RADIUS IETF attribute 5) will continue to be sent. If you do not want this information to be sent, you can suppress it by using the **no radius-server attribute nas-port** command. When this command is configured, the standard NAS-Port attribute will no longer be sent.

Examples

The following example specifies that RADIUS will display extended interface information:

```
radius-server vsa send
aaa nas port extended
```

Related Commands

Command	Description
radius-server extended-portnames	Displays expanded interface information in the NAS-Port attribute.
radius-server vsa send	Configures the network access server to recognize and use vendor-specific attributes.

aaa nas port option82

To send the remote-id and circuit-id as the NAS-Port-Id attribute in the Access-Request and Accounting-Request, use the **aaa nas port option82** command in global configuration mode. To disable this option, use the **no** form of this command.

aaa nas port option82

no aaa nas port option82

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2SB	This command was introduced in Cisco IOS Release 12.2SB.

Usage Guidelines

On platforms with multiple interfaces (ports) per slot, the Cisco RADIUS implementation will not provide a unique NAS-Port attribute that permits distinguishing between the interfaces. For example, if a dual PRI interface is in slot 1, calls on both Serial1/0:1 and Serial1/1:1 will appear as NAS-Port = 20101 due to the 16-bit field size limitation of the RADIUS IETF NAS-Port attribute.

In this case, the solution is to replace the NAS-Port attribute with the vendor-specific attribute (VSA) RADIUS IETF Attribute 26. The Cisco vendor ID is 9, and the Cisco-NAS-Port attribute is subtype 2. VSAs can be turned on by entering the **radius-server vsa send** command. The NAS-Port string information in this attribute is provided and configured using the **aaa nas port option82** command.

The standard NAS-Port attribute (RADIUS IETF attribute 5) will continue to be sent. If you do not want this information to be sent, you can suppress it by using the **no radius-server attribute nas-port** command. When this command is configured, the standard NAS-Port attribute will no longer be sent.

The NAS-Port information is populated in the Intelligent Service Gateway (ISG) interface that has received the DHCP **option82** packet. When the **aaa nas port option82** command is configured, the NAS-Port is populated with the information regarding the remote-id and circuit-id. If this command is not configured, the NAS-Port is populated with the local ISG NAS-Port-Id.

Examples

The following example specifies that RADIUS will display extended interface information:

```
radius-server vsa send
aaa nas port option82
```

Related Commands

Command	Description
radius-server vsa send	Configures the network access server to recognize and use VSAs.

aaa nas redirected-station

To include the original number in the information sent to the authentication server when the number dialed by a device is redirected to another number for authentication, use the **aaa nas redirected-station** command in global configuration mode. To leave the original number out of the information sent to the authentication server, use the **no** form of this command.

aaa nas redirected-station

no aaa nas redirected-station

Syntax Description

This command has no arguments or keywords.

Defaults

The original number is not included in the information sent to the authentication server.

Command Modes

Global configuration

Command History

Release	Modification
12.1 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If a customer is being authenticated by a RADIUS or TACACS+ server and the number dialed by the cable modem (or other device) is redirected to another number for authentication, the **aaa nas redirected-station** command will enable the original number to be included in the information sent to the authentication server.

This functionality allows the service provider to determine whether the customer dialed a number that requires special billing arrangements, such as a toll-free number.

The original number can be sent as a Cisco Vendor Specific Attribute (VSA) for TACACS+ servers and as RADIUS Attribute 93 (Ascend-Redirect-Number) for RADIUS servers. The RADIUS Attribute 93 is sent by default; to also send a VSA attribute for TACACS+ servers, use the **radius-server vsa send accounting** and **radius-server vsa send authentication** commands. To configure the RADIUS server to use RADIUS Attribute 93, add the non-standard option to the **radius-server host** command.

Note This feature is valid only when using port adapters that are configured for a T1 or E1 ISDN PRI or BRI interface. In addition, the telco switch performing the number redirection must be able to provide the redirected number in the Q.931 Digital Subscriber Signaling System Network Layer.

Examples

The following example enables the original number to be forwarded to the authentication server:

```
!
aaa authorization config-commands
aaa accounting exec default start-stop group radius
aaa accounting system default start-stop broadcast group apn23
aaa nas redirected-station
aaa session-id common
ip subnet-zero
!
```

Related Commands

Command	Description
radius-server host	Specifies a RADIUS server host.
radius-server vsa	Configures the network access server to recognize and use vendor-specific attributes.

aaa new-model

To enable the authentication, authorization, and accounting (AAA) access control model, issue the **aaa new-model** command in global configuration mode. To disable the AAA access control model, use the **no** form of this command.

aaa new-model

no aaa new-model

Syntax Description

This command has no arguments or keywords.

Command Default

AAA is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.4(4)T	Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2(33)SXI	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command enables the AAA access control system.

Examples

The following example initializes AAA:

```
aaa new-model
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication arap	Enables an AAA authentication method for ARAP using TACACS+.
aaa authentication enable default	Enables AAA authentication to determine if a user can access the privileged command level.
aaa authentication login	Sets AAA authentication at login.

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication method for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.

aaa password

To configure restrictions for an authentication, authorization, and accounting (AAA) password, use the **aaa password** command in in global configuration mode. To disable the password restriction, use the **no** form of this command.

aaa password restriction

no aaa password restriction

Syntax Description

restriction	Configures restrictions to the password.

Command Default

AAA passwords have no restrictions.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

The **aaa password** command can be used only if the **aaa new-model** command is configured. The restrictions are not applied to passwords in the startup configurations. The restrictions are not applied to passwords that already present in the configurations before the **aaa password** command is enabled.

Passwords are subject to the following restrictions:

- The new password must contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters.
- The new password should not have a character repeated more than three times consecutively.
- The new password should not be the same as the associated username. The password obtained by capitalization of the username or username reversed is not accepted.
- The new password should not be “cisco”, “ocsic”, or any variant obtained by changing the capitalization of letters therein, or by substituting “1” “|” or “!” for i, or by substituting “0” for “o”, or substituting “$” for “s”.

The restrictions can be applied to the passwords configured using the following commands: **aaa pod server**, **enable password**, **enable secret**, **radius-server key**, **radius-server host key**, **server-key**, and the **tacacs-server key**command.

Examples

The following example shows how to configure restrictions for an aaa password:

```
Router(config)# aaa password restriction
```

Related Commands

Command	Description
aaa pod server	Enables inbound user sessions to be disconnected when specific session attributes are presented.
enable password	Sets a local password to control access to various privilege levels.
enable secret	Specifies an additional layer of security over the enable password command.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
radius-server host	Specifies a RADIUS server host.
server-key	Configure the RADIUS key to be shared between a device and RADIUS clients.
tacacs-server host	Sets the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon.

aaa pod server

To enable inbound user sessions to be disconnected when specific session attributes are presented, use the **aaa pod server** command in global configuration mode. To disable the configuration, use the **no** form of this command.

aaa pod server [**clients** *ip-address1 ip-address2 ... ip-addressn*] [**port** *port-number*] {**auth-type** [**all ignore | any ignore**] **session-key server-key** *string* **| ignore** [**session-key**] **server-key | server-key** *string*}

no aaa pod server

Syntax Description

clients *ip-address*	(Optional) Registers the IP address of all the clients who can send POD requests. If this configuration is present and a POD request originates from a device that is not on the list, it is rejected. You can specify only four client IP addresses.
port *port number*	(Optional) Network access server User Datagram Protocol (UDP) port to use for packet of disconnect (POD) requests. Default value is 1700.
auth-type	Type of authorization required for disconnecting sessions. If no authentication type is specified, **auth-type** is the default.
all	(Optional) Only a session that matches all four key attributes is disconnected. The default is **all**.
any	(Optional) Session that matches all of the attributes sent in the POD packet is disconnected. The POD packet may contain one or more of four key attributes (user-name, framed-IP-address, session-ID, and session-key).
ignore	Ignores the session key or the server key received in the POD packet for session matching.
session-key	Session with a matching session-key attribute is disconnected. All other attributes are ignored.
server-key	Configures the shared-secret text string.
string	Shared-secret text string that is shared between the network access server and the client workstation. This shared-secret string must be the same on both systems.

Defaults

The POD server function is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(2)XH	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.

Release	Modification
12.2(2)XB	The *encryption-type* argument was added, as well as support for the voice applications and the Cisco 3600 series, and Cisco AS5350, and Cisco AS5400 routers.
12.2(2)XB1	Support for the Cisco AS5800 was added.
12.2(11)T	The *encryption-type* argument and support for the voice applications were added. **Note** Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800 is not included in this release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified. The **clients** and **ignore** keywords were added.

Usage Guidelines

To disconnect a session, the values in one or more of the key fields in the POD request must match the values for a session on one of the network access server ports. Which values must match depends on the **auth-type** attribute defined in the command. If no **auth-type** attribute is specified, all three values must match. If no match is found, all connections remain intact and an error response is returned. The key fields are as follows:

- An h323-conf-id vendor-specific attribute (VSA) with the same content as received from the gateway for this call.
- An h323-call-origin VSA with the same content as received from the gateway for the leg of interest.
- A 16-byte Message Digest 5 (MD5) hash value that is carried in the *authentication* field of the POD request.

Examples

The following example shows how to enable POD and set the secret key to “xyz123”:

```
aaa pod server server-key xyz123
```

Related Commands

Command	Description
aaa accounting delay-start	Delays generation of the start accounting record until the user IP address is established.
aaa accounting	Enables accounting records.
debug aaa pod	Displays debug messages for POD packets.
radius-server host	Identifies a RADIUS host.

aaa preauth

To enter authentication, authorization, and accounting (AAA) preauthentication configuration mode, use the **aaa preauth** command in global configuration mode. To disable preauthentication, use the **no** form of this command.

aaa preauth

no aaa preauth

Syntax Description

This command has no arguments or keywords.

Defaults

Preauthentication is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To enter AAA preauthentication configuration mode, use the **aaa preauth** command. To configure preauthentication, use a combination of the **aaa preauth** commands: **group**, **clid**, **ctype**, **dnis**, and **dnis bypass**. You must configure the **group** command. You must also configure one or more of the **clid**, **ctype**, **dnis**, or **dnis bypass** commands.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

You can use the **clid**, **ctype**, or **dnis** commands to define the list of the preauthentication elements. For each preauthentication element, you can also define options such as password (for all the elements, the default password is cisco). If you specify multiple elements, the preauthentication process will be performed on each element according to the order of the elements that you configure with the preauthentication commands. In this case, more than one RADIUS preauthentication profile is returned, but only the last preauthentication profile will be applied to the authentication and authorization later on, if applicable.

Examples

The following example enables dialed number identification service (DNIS) preauthentication using a RADIUS server and the password Ascend-DNIS:

```
aaa preauth
 dnis password Ascend-DNIS
```

Related Commands

Command	Description
dnis (authentication)	Enables AAA preauthentication using DNIS.
group (authentication)	Selects the security server to use for AAA preauthentication.
isdn guard-timer	Sets a guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request.

aaa processes

To allocate a specific number of background processes to be used to process authentication, authorization, and accounting (AAA) authentication and authorization requests for PPP, use the **aaa processes** command in global configuration mode. To restore the default value for this command, use the **no** form of this command.

aaa processes *number*

no aaa processes *number*

Syntax Description

number	Specifies the number of background processes allocated for AAA requests for PPP. Valid entries are 1 to 2147483647.

Defaults

The default for this command is one allocated background process.

Command Modes

Global configuration

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **aaa processes** command to allocate a specific number of background processes to simultaneously handle multiple AAA authentication and authorization requests for PPP. Previously, only one background process handled all AAA requests for PPP, so only one new user could be authenticated or authorized at a time. This command configures the number of processes used to handle AAA requests for PPP, increasing the number of users that can be simultaneously authenticated or authorized.

The argument *number* defines the number of background processes earmarked to process AAA authentication and authorization requests for PPP. This argument also defines the number of new users that can be simultaneously authenticated and can be increased or decreased at any time.

Examples

The following examples shows the **aaa processes** command within a standard AAA configuration. The authentication method list “dialins” specifies RADIUS as the method of authentication, then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP. Ten background processes have been allocated to handle AAA requests for PPP.

```
aaa new-model
aaa authentication ppp dialins group radius local
aaa processes 10
interface 5
```

```
encap ppp
ppp authentication pap dialins
```

Related Commands

Command	Description
show ppp queues	Monitors the number of requests processed by each AAA background process.

aaa route download

To enable the static route download feature and set the amount of time between downloads, use the **aaa route download** command in global configuration mode. To disable this function, use the **no** form of this command.

aaa route download [*time*] [**authorization** *method-list*]

no aaa route download

Syntax Description

time	(Optional) Time between downloads, in minutes. The range is from 1 to 1440 minutes.
authorization *method-list*	(Optional) Specify a named method list to which RADIUS authorization requests for static route downloads are sent. If these attributes are not set, all RADIUS authorization requests will be sent to the servers that are specified by the default method list.

Defaults

The default period between downloads (updates) is 720 minutes.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.1	This command was integrated into Cisco IOS Release 12.1.
12.2(8)T	The **authorization** keyword was added; the *method-list* argument was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

This command is used to download static route details from the authorization, authentication, and accounting (AAA) server if the name of the router is *hostname*. The name passed to the AAA server for static routes is *hostname-1*, *hostname-2*... *hostname-n*—the router downloads static routes until it fails an index and no more routes can be downloaded.

Examples

The following example sets the AAA route update period to 100 minutes:

```
aaa route download 100
```

The following example sets the AAA route update period to 10 minutes and sends static route download requests to the servers specified by the method list name “list1”:

```
aaa route download 10 authorization list1
```

Related Commands

Command	Description
aaa authorization configuration default	Downloads static route configuration information from the AAA server using TACACS+ or RADIUS.
clear ip route download	Clears static routes downloaded from a AAA server.
show ip route	Displays all static IP routes, or those installed using the AAA route download function.

aaa server radius dynamic-author

To configure a device as an authentication, authorization, and accounting (AAA) server to facilitate interaction with an external policy server, use the **aaa server radius dynamic-author** command in global configuration mode. To remove this configuration, use the **no** form of this command.

aaa server radius dynamic-author

no aaa server radius dynamic-author

Syntax Description

This command has no arguments or keywords.

Command Default

The device will not function as a server when interacting with external policy servers.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
12.2(5)SXI	This command was integrated into Cisco IOS Release 12.2(5)SXI.

Usage Guidelines

Dynamic authorization allows an external policy server to dynamically send updates to a device. Once the **aaa server radius dynamic-author** command is configured, dynamic authorization local server configuration mode is entered. Once in this mode, the RADIUS application commands can be configured.

Dynamic Authorization for the Intelligent Services Gateway (ISG)

ISG works with external devices, referred to as policy servers, that store per-subscriber and per-service information. ISG supports two models of interaction between the ISG device and external policy servers: initial authorization and dynamic authorization.

The dynamic authorization model allows an external policy server to dynamically send policies to the ISG. These operations can be initiated in-band by subscribers (through service selection) or through the actions of an administrator, or applications can change policies on the basis of an algorithm (for example, change session quality of service (QoS) at a certain time of day). This model is facilitated by the Change of Authorization (CoA) RADIUS extension. CoA introduced peer-to-peer capability to RADIUS, enabling ISG and the external policy server each to act as a RADIUS client and server.

Examples

The following example configures the ISG to act as a AAA server when interacting with the client at IP address 10.12.12.12:

```
aaa server radius dynamic-author
 client 10.12.12.12 key cisco
 message-authenticator ignore
```

Related Commands

Command	Description
auth-type (ISG)	Specifies the server authorization type.
client	Specifies a RADIUS client from which a device will accept CoA and disconnect requests.
default	Sets a RADIUS application command to its default.
domain	Specifies username domain options.
ignore	Overrides a behavior to ignore certain paremeters.
port	Specifies a port on which local RADIUS server listens.
server-key	Specifies the encryption key shared with RADIUS clients.

aaa service-profile

To configure the service profile parameters for an authentication, authorization, and accounting (AAA) session, use the **aaa service-profile** command in global configuration mode. To disable the service profile parameters for AAA sessions, use the **no** form of this command.

aaa service-profile key username-with-nasport

no aaa service-profile key username-with-nasport

Syntax Description

key	Assigns a key to save and search service profiles.
username-with-nasport	Configures the AAA server to use the username and network access server (NAS) port as the service profile key.

Command Default

Service profiles are stored based on the username.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Examples

The following example shows how to configure the service profile parameters for a AAA session:

```
Router# enable
Router# configure terminal
Router(config)# aaa service-profile key username-with-nasport
```

Related Commands

Command	Description
show aaa service-profiles	Displays the service profiles downloaded and stored by a AAA session.

aaa session-id

To specify whether the same session ID will be used for each authentication, authorization, and accounting (AAA) accounting service type within a call or whether a different session ID will be assigned to each accounting service type, use the **aaa session-id** command in global configuration mode. To restore the default behavior after the **unique** keyword is enabled, use the **no** form of this command.

aaa session-id [**common** | **unique**]

no aaa session-id [**unique**]

Syntax Description

common	(Optional) Ensures that all session identification (ID) information that is sent out for a given call will be made identical. The default behavior is **common**.
unique	(Optional) Ensures that only the corresponding service access-requests and accounting-requests will maintain a common session ID. Accounting-requests for each service will have a different session ID.

Defaults

The **common** keyword is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **common** keyword behavior allows the first session ID request of the call to be stored in a common database; all proceeding session ID requests will retrieve the value of the first session ID. Because a common session ID is the default behavior, this functionality is written to the system configuration after the **aaa new-model** command is configured.

Note The router configuration will always have either the **aaa session-id common** or the **aaa session-id unique** command enabled; it is not possible to have neither of the two enabled. Thus, the **no aaa session-id unique** command will revert to the default functionality, but the **no aaa session-id common** command will not have any effect because it is the default functionality.

The **unique** keyword behavior assigns a different session ID for each accounting type (Auth-Proxy, Exec, Network, Command, System, Connection, and Resource) during a call. To specify this behavior, the unique keyword *must* be specified. The session ID may be included in RADIUS access requests by configuring the **radius-server attribute 44 include-in-access-req** command. The session ID in the access-request will be the same as the session ID in the accounting request for the same service; all other services will provide unique session IDs for the same call.

Examples

The following example shows how to configure unique session IDs:

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server attribute 44 include-in-access-req
aaa session-id unique
```

Related Commands

Command	Description
aaa new model	Enables AAA.
radius-server attribute 44 include-in-access-req	Sends RADIUS attribute 44 (Accounting Session ID) in access request packets before user authentication (including requests for preauthentication).

aaa session-mib

To configure MIB options for Simple Network Management Protocol (SNMP) authentication, authorization, and accounting (AAA) sessions, use the **aaa session-mib** command in global configuration mode. To disable these options, use the **no** form of this command.

aaa session-mib {**disconnect** | **populate** {**setup** | **start**}}

no aaa session-mib {**disconnect** | **populate** {**setup** | **start**}}

Syntax Description

disconnect	Enables an AAA session MIB to disconnect authenticated clients using SNMP.
populate setup	Specifies that the AAA session MIB starts to track a session at the setup of the session.
populate start	Specifies that the AAA session MIB starts to track a session when accounting starts (when the START record is sent).

Command Default

No MIB options for SNMP AAA sessions are configured. OR IS THE DEFAULT “populate setup” AS DISCUSSED IN THE ‘Evaluation’ ATTACHMENT OF THE ENGINEERING DDTS (http://cdetsweb-prd.cisco.com/cdets/cli/ViewNote.html?identifier=CSCec12532&title=Evaluation)???

Command Modes

Global configuration (config)

Release	Modification
12.1(3)T	This command was introduced.
12.3(5)	The populate, setup and start keywords were added.
12.3(5a)B	The populate, setup and start keywords were added.
12.3(7)T	The populate, setup and start keywords were added.
12.2(16)BX3	The populate, setup and start keywords were added.
12.3(7)XI	The populate, setup and start keywords were added.
12.3(12)	The populate, setup and start keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **disconnect** keyword enables termination of authenticated client connections via SNMP. Without this keyword, a network management station cannot perform set operations and disconnect users (it can only poll the table).

The **populate** keyword determines when reporting of a locally terminated sessions begins. Two options are provided: **setup** (default) and **start**. The **setup** keyword begins tracking the session parameters during the setup of a session while the **start** keyword begins when the accounting START notification is generated and sent. By default, Cisco AAA session MIB begins reporting sessions generated during setup.

Examples

The following example shows how to enable the disconnection of authenticated clients using SNMP:

```
Router> enable
Router# configure terminal
Router(config)# aaa session-mib disconnect
```

The following example shows how to start tracking of a session at setup:

```
Router> enable
Router# configure terminal
Router(config)# aaa session-mib populate setup
```

aaa traceback recording

To enable traceback recording on an authentication, authorization, and accounting (AAA) server, use the **aaa traceback recording** command in global configuration mode. To disable the configuration, use the **no** form of this command.

aaa traceback recording

no aaa traceback recording

Syntax Description

This command has no arguments or keywords.

Command Default

Traceback recording is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows how to enable traceback recording on a AAA server:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa traceback recording
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.

aaa user profile

To create an authentication, authorization, and accounting (AAA) named user profile, use the **aaa user profile** command in global configuration mode. To remove a user profile from the configuration, use the **no** form of this command.

aaa user profile *profile-name*

no aaa user profile *profile-name*

Syntax Description

profile-name	Character string used to name the user profile. The maximum length of the character string is 63 characters. Longer strings will be truncated.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.3(3.8)	The maximum length of the *profile-name* argument is set at 63 characters.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Use the **aaa user profile** command to create a AAA user profile. Used in conjunction with the **aaa attribute** command, which adds calling line identification (CLID) and dialed number identification service (DNIS) attribute values, the user profile can be associated with the record that is sent to the RADIUS server (via the **test aaa group** command), which provides the RADIUS server with access to CLID or DNIS attribute information when the server receives a RADIUS record.

Examples

The following example shows how to configure a dnis = dnisvalue user profile named “prfl1”:

```
aaa user profile prfl1
 aaa attribute dnis
 aaa attribute dnis dnisvalue
 no aaa attribute clid
! Attribute not found.
 aaa attribute clid clidvalue
 no aaa attribute clid
```

Related Commands

Command	Description
aaa attribute	Adds DNIS or CLID attribute values to a user profile.
test aaa group	Associates a DNIS or CLID user profile with the record that is sent to the RADIUS server.

access (firewall farm)

To route specific flows to a firewall farm, use the **access** command in firewall farm configuration mode. To restore the default settings, use the **no** form of this command.

access [**source** *source-ip netmask* | **destination** *destination-ip netmask* | **inbound** *inbound-interface* | **outbound** *outbound-interface*]

no access [**source** *source-ip netmask* | **destination** *destination-ip netmask* | **inbound** *inbound-interface* | **outbound** *outbound-interface*]

Syntax Description

source	(Optional) Routes flows based on source IP address.
source-ip	(Optional) Source IP address. The default is 0.0.0.0 (all sources).
netmask	(Optional) Source IP network mask. The default is 0.0.0.0 (all source subnets).
destination	(Optional) Routes flows based on destination IP address.
destination-ip	(Optional) Destination IP address. The default is 0.0.0.0 (all destinations).
netmask	(Optional) Destination IP network mask. The default is 0.0.0.0 (all destination subnets).
inbound *inbound-interface*	(Optional) Indicates that the firewall farm is to accept inbound packets only on the specified inbound interface.
outbound *outbound-interface*	(Optional) Indicates that the firewall farm is to accept outbound packets only on the specified outbound interface.

Defaults

The default source IP address is 0.0.0.0 (routes flows from all sources to this firewall farm).
The default source IP network mask is 0.0.0.0 (routes flows from all source subnets to this firewall farm).
The default destination IP address is 0.0.0.0 (routes flows from all destinations to this firewall farm).
The default destination IP network mask is 0.0.0.0 (routes flows from all destination subnets to this firewall farm).
If you do not specify an inbound interface, the firewall farm accepts inbound packets on all inbound interfaces.
If you do not specify an outbound interface, the firewall farm accepts outbound packets on all outbound interfaces.

Command Modes

Firewall farm configuration (config-slb-fw)

Command History

Release	Modification
12.1(7)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	The **inbound** and **outbound** keywords and *inbound-interface* and *outbound-interface* arguments were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can specify more than one source or destination for each firewall farm. To do so, configure multiple **access** statements, making sure the network masks do not overlap each other.

You can specify up to two inbound interfaces and two outbound interfaces for each firewall farm. To do so, configure multiple **access** statements, keeping the following considerations in mind:

- All inbound and outbound interfaces must be in the same Virtual Private Network (VPN) routing and forwarding (VRF).
- All inbound and outbound interfaces must be different from each other.
- You cannot change inbound or outbound interfaces for a firewall farm while it is in service.

Examples

The following example routes flows with a destination IP address of 10.1.6.0 to firewall farm FIRE1:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# access destination 10.1.6.0 255.255.255.0
```

Related Commands

Command	Description
show ip slb firewallfarm	Displays information about the firewall farm configuration.

access (server farm)

To configure an access interface for a server farm, use the **access** command in server farm configuration mode. To disable the access interface, use the **no** form of this command.

access *interface*

no access *interface*

Syntax Description

interface	Interface to be inspected. The server farm will handle outbound flows from real servers only on the specified interface.

Defaults

The server farm handles outbound flows from real servers on all interfaces.

Command Modes

Server farm configuration (config-slb-sfarm)

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The virtual server and its associated server farm interfaces must be in the same Virtual Private Network (VPN) routing and forwarding (VRF).

You can specify up to two access interfaces for each server farm. To do so, configure two **access** statements, keeping the following considerations in mind:

- The two interfaces must be in the same VRF.
- The two interfaces must be different from each other.
- The access interfaces of primary and backup server farms must be the same.
- You cannot change the interfaces for a server farm while it is in service.

Examples

The following example limits the server farm to handling outbound flows from real servers only on access interface Vlan106:

```
Router(config)# ip slb serverfarm SF1
Router(config-slb-sfarm)# access Vlan106
```

Related Commands

Command	Description
show ip slb serverfarms	Displays information about the server farms.

access (virtual server)

To enable framed-IP routing to inspect the ingress interface, use the **access** command in virtual server configuration mode. To disable framed-IP routing, use the **no** form of this command.

access *interface* [**route framed-ip**]

no access *interface* [**route framed-ip**]

Syntax Description

interface	Interface to be inspected.
route framed-ip	(Optional) Routes flows using framed-IP routing.

Defaults

Framed-IP routing cannot inspect the ingress interface.

Command Modes

Virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.1(12c)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	The command was modified to accept up to two framed-IP access interfaces (specified on separate commands).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command enables framed-IP routing to inspect the ingress interface when routing subscriber traffic. All framed-IP sticky database entries created as a result of RADIUS requests to this virtual server will include the interface in the entry. In addition to matching the source IP address of the traffic with the framed-IP address, the ingress interface must also match this interface when this command is configured.

You can use this command to allow subscriber data packets to be routed to multiple service gateway service farms.

The virtual server and its associated server farm interfaces must be in the same Virtual Private Network (VPN) routing and forwarding (VRF).

You can specify up to two framed-IP access interfaces for each virtual server. To do so, configure two **access** statements, keeping the following considerations in mind:

- The two interfaces must be in the same VRF.
- The two interfaces must be different from each other.
- You cannot change the interfaces for a virtual server while it is in service.

Examples

The following example enables framed-IP routing to inspect ingress interface Vlan20:

```
Router(config)# ip slb vserver SSG_AUTH
Router(config-slb-vserver)# access Vlan20 route framed-ip
```

Related Commands

Command	Description
show ip slb vservers	Displays information about the virtual servers defined to IOS SLB.

access-class

To restrict incoming and outgoing connections between a particular vty (into a Cisco device) and the addresses in an access list, use the **access-class** command in line configuration mode. To remove access restrictions, use the **no** form of this command.

access-class *access-list-number* {**in** [**vrf-also**] | **out**}

no access-class *access-list-number* {**in** | **out**}

Syntax Description

access-list-number	Number of an IP access list. This is a decimal number from 1 to 199 or from 1300 to 2699.
in	Restricts incoming connections between a particular Cisco device and the addresses in the access list.
vrf-also	(Optional) Accepts incoming connections from interfaces that belong to a VRF.
out	Restricts outgoing connections between a particular Cisco device and the addresses in the access list.

Defaults

No access lists are defined.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2	The **vrf-also** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Remember to set identical restrictions on all the virtual terminal lines because a user can connect to any of them.

To display the access lists for a particular terminal line, use the **show line** EXEC command and specify the line number.

If you do not specify the **vrf-also** keyword, incoming Telnet connections from interfaces that are part of a VRF are rejected.

Examples

The following example defines an access list that permits only hosts on network 192.89.55.0 to connect to the virtual terminal ports on the router:

```
access-list 12 permit 192.89.55.0 0.0.0.255
```

```
 line 1 5
 access-class 12 in
```

The following example defines an access list that denies connections to networks other than network 10.0.0.0 on terminal lines 1 through 5:

```
access-list 10 permit 10.0.0.0 0.255.255.255
 line 1 5
 access-class 10 out
```

Related Commands

Command	Description
show line	Displays the parameters of a terminal line.

access-enable

To enable the router to create a temporary access list entry in a dynamic access list, use the **access-enable** command in EXEC mode.

access-enable [**host**] [**timeout** *minutes*]

Syntax Description

host	(Optional) Tells the software to enable access only for the host from which the Telnet session originated. If not specified, the software allows all hosts on the defined network to gain access. The dynamic access list contains the network mask to use for enabling the new network.
timeout *minutes*	(Optional) Specifies an idle timeout for the temporary access list entry. If the access list entry is not accessed within this period, it is automatically deleted and requires the user to authenticate again. The default is for the entries to remain permanently. We recommend that this value equal the idle timeout set for the WAN connection.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command enables the lock-and-key access feature.

You should always define either an idle timeout (with the **timeout** keyword in this command) or an absolute timeout (with the **timeout** keyword in the **access-list** command). Otherwise, the temporary access list entry will remain, even after the user terminates the session.

Use the **autocommand** command with the **access-enable** command to cause the **access-enable** command to execute when a user opens a Telnet session into the router.

Examples

The following example causes the software to create a temporary access list entry and tells the software to enable access only for the host from which the Telnet session originated. If the access list entry is not accessed within 2 minutes, it is deleted.

```
autocommand access-enable host timeout 2
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
autocommand	Configures the Cisco IOS software to automatically execute a command when a user connects to a particular line.
show ip accounting	Displays the active accounting or checkpointed database or displays access list violations.

access-group (identity policy)

To specify an access group to be applied to an identity policy, use the **access-group** command in identity policy configuration mode. To remove the access group, use the **no** form of this command.

access-group *group-name*

no access-group *group-name*

Syntax Description

group-name	Access list name.

Defaults

An access group is not specified.

Command Modes

Identity policy configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Using this command, you can access only named access lists.

Examples

The following example shows that access group "exempt-acl" is to be applied to the identity policy "policyname1":

```
Router (config)# identity policy policyname1
Router (config-identity-policy)# access-group exempt-acl
```

Related Commands

Command	Description
identity profile	Creates an identity profile.

access-group mode

To specify the override modes (for example, VLAN ACL [VACL] overrides Port ACL [PACL]) and the nonoverride modes (for example, merge or strict mode) for an access group, use the **access-group mode** command in interface configuration mode. To return to preferred port mode, use the **no** form of this command.

access-group mode {**prefer** {**port** | **vlan**} | **merge**}

no access-group mode {**prefer** {**port** | **vlan**} | **merge**}

Syntax Description

prefer port	Specifies that the PACL mode take precedence if PACLs are configured. If no PACL features are configured on the port, other features applicable to the interface are merged and applied on the interface.
prefer vlan	Specifies that the VLAN-based ACL mode take precedence. If no VLAN-based ACL features are configured on the port's VLAN, the PACL features on the port are applied.
merge	Merges applicable ACL features before they are programmed into the hardware.

Command Default

The default is **port** ACL override mode.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

On the Layer 2 interface, prefer port, prefer VLAN, and merge modes are supported. A Layer 2 interface can have one IP ACL applied in either direction (one inbound and one outbound).

Examples

This example shows how to configure an interface to use prefer port mode:

```
Router(config-if)# access-group mode prefer port
```

This example shows how to configure an interface to use merge mode:

```
Router(config-if)# access-group mode merge
```

Related Commands

Command	Description
show access-group mode interface	Displays the ACL configuration on a Layer 2 interface.

access-list (IP extended)

To define an extended IP access list, use the extended version of the **access-list** command in global configuration mode. To remove the access lists, use the **no** form of this command.

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**time-range** *time-range-name*] [**fragments**] [**log** [*word*] | **log-input** [*word*]]

no access-list *access-list-number*

Internet Control Message Protocol (ICMP)

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* [*icmp-code*] | *icmp-message*] [**precedence** *precedence*] [**tos** *tos*] [**time-range** *time-range-name*] [**fragments**] [**log** [*word*] | **log-input** [*word*]]

Internet Group Management Protocol (IGMP)

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**time-range** *time-range-name*] [**fragments**] [**log** [*word*] | **log-input** [*word*]]

Transmission Control Protocol (TCP)

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} **tcp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**time-range** *time-range-name*] [**fragments**] [**log** [*word*] | **log-input** [*word*]]

User Datagram Protocol (UDP)

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} **udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**time-range** *time-range-name*] [**fragments**] [**log** [*word*] | **log-input** [*word*]]

Syntax Description

access-list-number	Number of an access list. This is a decimal number from 100 to 199 or from 2000 to 2699.
dynamic *dynamic-name*	(Optional) Identifies this access list as a dynamic access list. Refer to lock-and-key access documented in the "Configuring Lock-and-Key Security (Dynamic Access Lists)" chapter in the *Cisco IOS Security Configuration Guide*.
timeout *minutes*	(Optional) Specifies the absolute length of time, in minutes, that a temporary access list entry can remain in a dynamic access list. The default is an infinite length of time and allows an entry to remain permanently. Refer to lock-and-key access documented in the "Configuring Lock-and-Key Security (Dynamic Access Lists)" chapter in the *Cisco IOS Security Configuration Guide*.

deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
protocol	Name or number of an Internet protocol. It can be one of the keywords **eigrp**, **gre**, **icmp**, **igmp**, **ip**, **ipinip**, **nos**, **ospf**, **pim**, **tcp**, or **udp**, or an integer in the range from 0 to 255 representing an Internet protocol number. To match any Internet protocol (including ICMP, TCP, and UDP) use the **ip** keyword. Some protocols allow further qualifiers described below.
source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part dotted decimal format. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** source as an abbreviation for a *source* and *source-wildcard* of source 0.0.0.0.
source-wildcard	Wildcard bits to be applied to source. Each wildcard bit 0 indicates the corresponding bit position in the source. Each wildcard bit set to 1 indicates that both a 0 bit and a 1 bit in the corresponding position of the IP address of the packet will be considered a match to this access list entry. There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part dotted decimal format. Place 1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0. Wildcard bits set to 1 need not be contiguous in the source wildcard. For example, a source wildcard of 0.255.0. would be valid.
destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part dotted decimal format. • Use the **any** keyword as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of destination 0.0.0.0.
destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part dotted decimal format. Place 1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** destination as an abbreviation for a *destination* and *destination-wildcard* of destination 0.0.0.0.

precedence *precedence*	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7, or by name as listed in the section "Usage Guidelines."
tos *tos*	(Optional) Packets can be filtered by type of service level, as specified by a number from 0 to 15, or by name as listed in the section "Usage Guidelines."
time-range *time-range-name*	(Optional) Name of the time range that applies to this statement. The name of the time range and its restrictions are specified by the **time-range** command.
icmp-type	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
icmp-code	(Optional) ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
icmp-message	(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name. The possible names are listed in the section "Usage Guidelines."
igmp-type	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the section "Usage Guidelines."
operator	(Optional) Compares source or destination ports. Possible operands include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source* and *source-wildcard*, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard*, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number.
port	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the section "Usage Guidelines." TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP. TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST control bits set. The nonmatching case is that of the initial TCP datagram to form a connection.
fragments	(Optional) The access list entry applies to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the "Access List Processing of Fragments" and "Fragments and Policy Routing" sections in the "Usage Guidelines" section.

log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The log message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and if appropriate, the source and destination addresses and port numbers and the user-defined cookie or router-generated hash value. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. The logging facility may drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list. After you specify the **log** keyword (and the associated *word* argument), you cannot specify any other keywords or settings for this command.
word	(Optional) User-defined cookie appended to the log message. The cookie: • cannot be more than characters • cannot start with hexadecimal notation (such as 0x) • cannot be the same as, or a subset of, the following keywords: **reflect**, **fragment**, **time-range** • must contain alphanumeric characters only The user-defined cookie is appended to the access control entry (ACE) syslog entry and uniquely identifies the ACE, within the access control list, that generated the syslog entry.
log-input	(Optional) Includes the input interface and source MAC address or virtual circuit in the logging output. After you specify the **log-input** keyword (and the associated *word* argument), you cannot specify any other keywords or settings for this command.

Defaults

An extended access list defaults to a list that denies everything. An extended access list is terminated by an implicit deny statement.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
10.3	The following keywords and arguments were added: • *source* • *source-wildcard* • *destination* • *destination-wildcard* • **precedence** *precedence* • *icmp-type* • *icmp-code* • *icmp-message* • *igmp-type* • *operator* • *port* • **established**
11.1	The **dynamic** *dynamic-name* keyword and argument were added.
11.1	The **timeout** *minutes* keyword and argument were added.
11.2	The **log-input** keyword was added.
12.0(1)T	The **time-range** *time-range-name* keyword and argument were added.
12.0(11)	The **fragments** keyword was added.
12.2(13)T	The **non500-isakmp** keyword was added to the list of UDP port names. The **igrp** keyword was removed because the IGRP protocol is no longer available in Cisco IOS software.
12.4	The **drip** keyword was added to specify the TCP port number used for OER communication.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(22)T	The *word* argument was added to the **log** and **log-input** keywords.

Usage Guidelines

You can use access lists to control the transmission of packets on an interface, control vty access, and restrict the contents of routing updates. The Cisco IOS software stops checking the extended access list after a match occurs.

Fragmented IP packets, other than the initial fragment, are immediately accepted by any extended IP access list. Extended access lists used to control vty access or restrict the contents of routing updates must not match against the TCP source port, the type of service (ToS) value, or the precedence of the packet.

Note After a numbered access list is created, any subsequent additions (possibly entered from the terminal) are placed at the end of the list. In other words, you cannot selectively add or remove access list command lines from a specific numbered access list.

The following is a list of precedence names:

- **critical**
- **flash**
- **flash-override**
- **immediate**
- **internet**
- **network**
- **priority**
- **routine**

The following is a list of ToS names:

- **max-reliability**
- **max-throughput**
- **min-delay**
- **min-monetary-cost**
- **normal**

The following is a list of ICMP message type and code names:

- **administratively-prohibited**
- **alternate-address**
- **conversion-error**
- **dod-host-prohibited**
- **dod-net-prohibited**
- **echo**
- **echo-reply**
- **general-parameter-problem**
- **host-isolated**
- **host-precedence-unreachable**
- **host-redirect**
- **host-tos-redirect**
- **host-tos-unreachable**
- **host-unknown**
- **host-unreachable**
- **information-reply**
- **information-request**
- **mask-reply**

- **mask-request**
- **mobile-redirect**
- **net-redirect**
- **net-tos-redirect**
- **net-tos-unreachable**
- **net-unreachable**
- **network-unknown**
- **no-room-for-option**
- **option-missing**
- **packet-too-big**
- **parameter-problem**
- **port-unreachable**
- **precedence-unreachable**
- **protocol-unreachable**
- **reassembly-timeout**
- **redirect**
- **router-advertisement**
- **router-solicitation**
- **source-quench**
- **source-route-failed**
- **time-exceeded**
- **timestamp-reply**
- **timestamp-request**
- **traceroute**
- **ttl-exceeded**
- **unreachable**

The following is a list of IGMP message names:

- **dvmrp**
- **host-query**
- **host-report**
- **pim**
- **trace**

The following is a list of TCP port names that can be used instead of port numbers. Refer to the current assigned numbers RFC to find a reference to these protocols. Port numbers corresponding to these protocols can also be found if you type a ? in the place of a port number.

- **bgp**
- **chargen**
- **daytime**

- **discard**
- **domain**
- **drip**
- **echo**
- **finger**
- **ftp**
- **ftp-data**
- **gopher**
- **hostname**
- **irc**
- **klogin**
- **kshell**
- **lpd**
- **nntp**
- **pop2**
- **pop3**
- **smtp**
- **sunrpc**
- **syslog**
- **tacacs-ds**
- **talk**
- **telnet**
- **time**
- **uucp**
- **whois**
- **www**

The following is a list of UDP port names that can be used instead of port numbers. Refer to the current assigned numbers RFC to find a reference to these protocols. Port numbers corresponding to these protocols can also be found if you type a ? in the place of a port number.

- **biff**
- **bootpc**
- **bootps**
- **discard**
- **dnsix**
- **domain**
- **echo**
- **mobile-ip**
- **nameserver**

- **netbios-dgm**
- **netbios-ns**
- **non500-isakmp**
- **ntp**
- **rip**
- **snmp**
- **snmptrap**
- **sunrpc**
- **syslog**
- **tacacs-ds**
- **talk**
- **tftp**
- **time**
- **who**
- **xdmcp**

Access List Processing of Fragments

The behavior of access-list entries regarding the use or lack of the **fragments** keyword can be summarized as follows:

If the Access-List Entry has...	Then..
...no **fragments** keyword (the default behavior), and assuming all of the access-list entry information matches,	For an access-list entry containing only Layer 3 information: • The entry is applied to nonfragmented packets, initial fragments and noninitial fragments. For an access list entry containing Layer 3 and Layer 4 information: • The entry is applied to nonfragmented packets and initial fragments. – If the entry is a **permit** statement, the packet or fragment is permitted. – If the entry is a **deny** statement, the packet or fragment is denied. • The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access-list entry can be applied. If the Layer 3 portion of the access-list entry matches, and – If the entry is a **permit** statement, the noninitial fragment is permitted. – If the entry is a **deny** statement, the next access-list entry is processed. **Note** The **deny** statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.
...the **fragments** keyword, and assuming all of the access-list entry information matches,	The access-list entry is applied only to noninitial fragments. **Note** The **fragments** keyword cannot be configured for an access-list entry that contains any Layer 4 information.

Be aware that you should not simply add the **fragments** keyword to every access list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments** keyword, the packet is compared to the next access list entry, and so on, until it is either permitted or denied by an access list entry that does not contain the **fragments** keyword. Therefore, you may need two access list entries for every **deny** entry. The first **deny** entry of the pair will not include the **fragments** keyword, and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases where there are multiple **deny** access list entries for the same host but with different Layer 4 ports, a single **deny** access-list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets and each counts individually as a packet in access list accounting and access list violation counts.

Note The **fragments** keyword cannot solve all cases involving access lists and IP fragments.

Fragments and Policy Routing

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip address** command and the access list had entries that match on Layer 4 through 7 information. It is possible that noninitial fragments pass the access list and are policy routed, even if the first fragment was not policy routed or the reverse.

By using the **fragments** keyword in access list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made and it is more likely policy routing will occur as intended.

Permitting Optimized Edge Routing (OER) Communication

The **drip** keyword was introduced under the **tcp** keyword to support packet filtering in a network where OER is configured. The **drip** keyword specifies port 3949 that OER uses for internal communication. This option allows you to build a packet filter that permits communication between an OER master controller and border router(s). The **drip** keyword is entered following the TCP source, destination, and the **eq** operator. See the example at the end of this command reference page.

Examples

In the following example, serial interface 0 is part of a Class B network with the address 10.88.0.0, and the address of the mail host is 10.88.1.2. The **established** keyword is used only for the TCP protocol to indicate an established connection. A match occurs if the TCP datagram has the ACK or RST bits set, which indicates that the packet belongs to an existing connection.

```
access-list 102 permit tcp 0.0.0.0 255.255.255.255 10.88.0.0 0.0.255.255 established
access-list 102 permit tcp 0.0.0.0 255.255.255.255 10.88.1.2 0.0.0.0 eq 25
interface serial 0
 ip access-group 102 in
```

The following example permits Domain Naming System (DNS) packets and ICMP echo and echo reply packets:

```
access-list 102 permit tcp any 10.88.0.0 0.0.255.255 established
access-list 102 permit tcp any host 10.88.1.2 eq smtp
access-list 102 permit tcp any any eq domain
access-list 102 permit udp any any eq domain
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
```

The following examples show how wildcard bits are used to indicate the bits of the prefix or mask that are relevant. Wildcard bits are similar to the bitmasks that are used with normal access lists. Prefix or mask bits corresponding to wildcard bits set to 1 are ignored during comparisons and prefix or mask bits corresponding to wildcard bits set to 0 are used in comparison.

The following example permits 192.168.0.0 255.255.0.0 but denies any more specific routes of 192.168.0.0 (including 192.168.0.0 255.255.255.0):

```
access-list 101 permit ip 192.168.0.0 0.0.0.0   255.255.0.0 0.0.0.0
access-list 101 deny ip 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255
```

The following example permits 10.108.0/24 but denies 10.108/16 and all other subnets of 10.108.0.0:

```
access-list 101 permit ip 10.108.0.0 0.0.0.0     255.255.255.0 0.0.0.0
access-list 101 deny ip 10.108.0.0 0.0.255.255 255.255.0.0   0.0.255.255
```

The following example uses a time range to deny HTTP traffic on Monday through Friday from 8:00 a.m. to 6:00 p.m.:

```
time-range no-http
 periodic weekdays 8:00 to 18:00
!
access-list 101 deny tcp any any eq http time-range no-http
!
interface ethernet 0
 ip access-group 101 in
```

The following example permits communication, from any TCP source and destination, between an OER master controller and border router:

```
access-list 100 permit tcp any eq drip any eq drip
```

The following example shows how to configure the access list with the **log** keyword. It sets the *word* argument to UserDefinedValue. The word UserDefinedValue is appended to the related syslog entry:

```
Router(config)# access-list 101 permit tcp host 10.1.1.1 host 10.1.1.2 log
UserDefinedValue
```

Related Commands

Command	Description
access-class	Restricts incoming and outgoing connections between a particular vty (into a Cisco device) and the addresses in an access list.
access-list (IP standard)	Defines a standard IP access list.
access-list remark	Writes a helpful comment (remark) for an entry in a numbered IP access list.
clear access-template	Clears a temporary access list entry from a dynamic access list.
delay (tracking)	Sets conditions under which a packet does not pass a named access list.
distribute-list in (IP)	Filters networks received in updates.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
ip access-group	Controls access to an interface.
ip access-list	Defines an IP access list by name.
ip access-list logging hash-generation	Enables hash value generation for ACE syslog entries.
ip accounting	Enables IP accounting on an interface.
logging console	Controls which messages are logged to the console, based on severity.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list.
permit (IP)	Sets conditions under which a packet passes a named access list.
remark	Writes a helpful comment (remark) for an entry in a named IP access list.
show access-lists	Displays the contents of current IP and rate-limit access lists.
show ip access-list	Displays the contents of all current IP access lists.
time-range	Specifies when an access list or other feature is in effect.

access-list (IP standard)

To define a standard IP access list, use the standard version of the **access-list** command in global configuration mode. To remove a standard access list, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log** [*word*]]

no access-list *access-list-number*

Syntax Description

access-list-number	Number of an access list. This is a decimal number from 1 to 99 or from 1300 to 1999.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
source	Number of the network or host from which the packet is being sent. There are two alternative ways to specify the source: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
source-wildcard	(Optional) Wildcard bits to be applied to the source. There are two alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place 1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The log message includes the access list number, whether the packet was permitted or denied, the source address, the number of packets, and if appropriate, the user-defined cookie or router-generated hash value. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.

word	(Optional) User-defined cookie appended to the log message. The cookie: • cannot be more than characters • cannot start with hexadecimal notation (such as 0x) • cannot be the same as, or a subset of, the following keywords: **reflect**, **fragment**, **time-range** • must contain alphanumeric characters only The user-defined cookie is appended to the access control entry (ACE) syslog entry and uniquely identifies the ACE, within the access control list, that generated the syslog entry.

Defaults

The access list defaults to an implicit deny statement for everything. The access list is always terminated by an implicit deny statement for everything.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
11.3(3)T	The **log** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(22)T	The *word* argument was added to the **log** keyword.

Usage Guidelines

Plan your access conditions carefully and be aware of the implicit deny statement at the end of the access list.

You can use access lists to control the transmission of packets on an interface, control vty access, and restrict the contents of routing updates.

Use the **show access-lists** EXEC command to display the contents of all access lists.

Use the **show ip access-list** EXEC command to display the contents of one access list.

Caution Enhancements to this command are backward compatible; migrating from releases prior to Cisco IOS Release 10.3 will convert your access lists automatically. However, releases prior to Release 10.3 are not upwardly compatible with these enhancements. Therefore, if you save an access list with these images and then use software prior to Release 10.3, the resulting access list will not be interpreted correctly. **This condition could cause you severe security problems.** Save your old configuration file before booting these images.

Examples

The following example of a standard access list allows access for only those hosts on the three specified networks. The wildcard bits apply to the host portions of the network addresses. Any host with a source address that does not match the access list statements will be rejected.

```
access-list 1 permit 192.168.34.0 0.0.0.255
access-list 1 permit 10.88.0.0 0.0.255.255
access-list 1 permit 10.0.0.0 0.255.255.255
! (Note: all other access implicitly denied)
```

The following example of a standard access list allows access for devices with IP addresses in the range from 10.29.2.64 to 10.29.2.127. All packets with a source address not in this range will be rejected.

```
access-list 1 permit 10.29.2.64 0.0.0.63
! (Note: all other access implicitly denied)
```

To specify a large number of individual addresses more easily, you can omit the wildcard if it is all zeros. Thus, the following two configuration commands are identical in effect:

```
access-list 2 permit 10.48.0.3
access-list 2 permit 10.48.0.3 0.0.0.0
```

The following example of a standard access list allows access for devices with IP addresses in the range from 10.29.2.64 to 10.29.2.127. All packets with a source address not in this range will be rejected.

```
access-list 1 permit 10.29.2.64 0.0.0.63
! (Note: all other access implicitly denied)
```

The following example of a standard access list allows access for devices with IP addresses in the range from 10.29.2.64 to 10.29.2.127. All packets with a source address not in this range will be rejected. In addition, the logging mechanism is enabled and the word SampleUserValue is appended to each syslog entry.

```
Router(config)# access-list 1 permit 10.29.2.64 0.0.0.63 log SampleUserValue
```

Related Commands

Command	Description
access-class	Restricts incoming and outgoing connections between a particular vty (into a Cisco device) and the addresses in an access list.
access-list (IP extended)	Defines an extended IP access list.
access-list remark	Writes a helpful comment (remark) for an entry in a numbered IP access list.
deny (IP)	Sets conditions under which a packet does not pass a named access list.
distribute-list in (IP)	Filters networks received in updates.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
ip access-group	Controls access to an interface.
ip access-list logging hash-generation	Enables hash value generation for ACE syslog entries.
permit (IP)	Sets conditions under which a packet passes a named access list.
remark (IP)	Writes a helpful comment (remark) for an entry in a named IP access list.
show access-lists	Displays the contents of current IP and rate-limit access lists.
show ip access-list	Displays the contents of all current IP access lists.

access-list (NLSP)

To define an access list that denies or permits area addresses that summarize routes, use the NetWare Link-Services Protocol (NLSP) route aggregation version of the **access-list** command in global configuration mode. To remove an NLSP route aggregation access list, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} *network network-mask* [*interface*] [**ticks** *ticks*] [**area-count** *area-count*]

no access-list *access-list-number* {**deny** | **permit**} *network network-mask* [*interface*] [**ticks** *ticks*] [**area-count** *area-count*]

Syntax Description

access-list-number	Number of the access list. This is a number from 1200 to 1299.
deny	Denies redistribution of explicit routes if the conditions are matched. If you have enabled route summarization with route-aggregation command, the router redistributes an aggregated route instead.
permit	Permits redistribution of explicit routes if the conditions are matched.
network	Network number to summarize. An IPX network number is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
network-mask	Specifies the portion of the network address that is common to all addresses in the route summary. The high-order bits of *network-mask* must be contiguous Fs, while the low-order bits must be contiguous zeros (0). An arbitrary mix of Fs and 0s is not permitted.
interface	(Optional) Interface on which the access list should be applied to incoming updates.
ticks *ticks*	(Optional) Metric assigned to the route summary. The default is 1 tick.
area-count *area-count*	(Optional) Maximum number of NLSP areas to which the route summary can be redistributed. The default is 6 areas.

Defaults

No access lists are predefined.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.0	The *interface* argument was added.

Release	Modification
12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in12.2S-Family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the NLSP route aggregation access list in the following situations:

- When redistributing from an Enhanced IGRP or RIP area into a new NLSP area.

  Use the access list to instruct the router to redistribute an aggregated route instead of the explicit route. The access list also contains a "permit all" statement that instructs the router to redistribute explicit routes that are not subsumed by a route summary.

- When redistributing from an NLSP version 1.0 area into an NLSP version 1.1 area, and vice versa.

  From an NLSP version 1.0 area into an NLSP version 1.1 area, use the access list to instruct the router to redistribute an aggregated route instead of an explicit route and to redistribute explicit routes that are not subsumed by a route summary.

  From an NLSP version 1.1 area into an NLSP version 1.0 area, use the access list to instruct the router to filter aggregated routes from passing into the NLSP version 1.0 areas and to redistribute explicit routes instead.

Note NLSP version 1.1 routers refer to routers that support the route aggregation feature, while NLSP version 1.0 routers refer to routers that do not.

Examples

The following example uses NLSP route aggregation access lists to redistribute routes learned from RIP to NLSP area1. Routes learned via RIP are redistributed into NLSP area1. Any routes learned via RIP that are subsumed by aaaa0000 ffff0000 are not redistributed. An address summary is generated instead.

```
ipx routing
ipx internal-network 2000

interface ethernet 1
 ipx network 1001
 ipx nlsp area1 enable

interface ethernet 2
 ipx network 2001

access-list 1200 deny aaaa0000 ffff0000
access-list 1200 permit -1

ipx router nlsp area
 area-address 1000 fffff000
 route-aggregation
 redistribute rip access-list 1200
```

Related Commands

Command	Description
area-address (NLSP)	Defines a set of network numbers to be part of the current NLSP area.
deny (NLSP)	Filters explicit routes and generates an aggregated route for a named NLSP route aggregation access list.
ipx access-list	Defines an IPX access list by name.
ipx nlsp enable	Configures the interval between the transmission of hello packets.
ipx router	Specifies the routing protocol to use.
permit (NLSP)	Allows explicit route redistribution in a named NLSP route aggregation access list.
prc-interval	Controls the hold-down period between partial route calculations.
redistribute (IPX)	Redistributes from one routing domain into another.

access-list compiled

To enable the Turbo Access Control Lists (Turbo ACL) feature, use the **access-list compiled** command in global configuration mode. To disable the Turbo ACL feature, use the **no** form of this command.

access-list compiled

no access-list compiled

Syntax Description

This command has no arguments or keywords.

Defaults

Turbo ACL is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(6)S	This command was introduced.
12.1(1)E	This command was introduced for Cisco 7200 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(4)E	This command was implemented on the Cisco 7100 series.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

By default, the Turbo ACL feature is disabled. When Turbo ACL is disabled, normal ACL processing is enabled, and no ACL acceleration occurs.

When the Turbo ACL feature is enabled using the **access-list compiled** command, the ACLs in the configuration are scanned and, if suitable, compiled for Turbo ACL acceleration. This scanning and compilation may take a few seconds when the system is processing large and complex ACLs, or when the system is processing a configuration that contains a large number of ACLs.

Any configuration change to an ACL that is being accelerated, such as the addition of new ACL entries or the deletion of the ACL, triggers a recompilation of that ACL.

When Turbo ACL tables are being built (or rebuilt) for a particular ACL, the normal sequential ACL search is used until the new tables are ready for installation.

Examples

The following example enables the Turbo ACL feature:

```
access-list compiled
```

access-list compiled data-link limit memory

To change the amount of memory reserved for Turbo ACL processing for Layer 2 traffic in the Route Processor path for a Cisco 7304 router using a network services engine (NSE), use the **access-list compiled data-link limit memory** command in global configuration mode. To place no restrictions on the amount of memory reserved for Turbo ACL processing of Layer 2 traffic in the Route Processor path for a Cisco 7304 router using an NSE, use the **no** form of this command. To restore the default amount of memory reserved for Turbo ACL processing for Layer 2 traffic in the Route Processor path for a Cisco 7304 router using an NSE, use the **default** form of this command.

access-list compiled data-link limit memory *number*

no access-list compiled data-link limit memory

default access-list compiled data-link limit memory

Syntax Description

number	A number between 8 and 4095 that specifies the amount of memory, in megabytes, reserved for Turbo ACL processing of Layer 2 traffic in the Route Processor path for the Cisco 7304 router using an NSE.

Command Default

The default for *number* is 128.

Command Modes

Global configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced.

Usage Guidelines

The **show access-list compiled** command output provides information useful in helping to consider the exact memory limit to configure. The following sections of the **show access-list compiled** output, which are found in the "Compiled ACL statistics for Data-Link" section of the output, are especially useful:

- The "mem limits" output shows the number of times a compile has occurred and the ACL has reached its configured limit.
- The "Mb limit" output shows the current memory limit setting.
- The "Mb max memory" output shows the maximum amount of memory the current ACL configuration could actually consume under maximum usage conditions.

Note that there is a direct trade-off between memory used for ACL processing in the RP path and the memory used for other RP processes. Memory reserved for ACL processing cannot be used for other RP processes, and vice versa. If you need more memory for ACL processing, you should set a higher value for *number*. If you need more memory for other RP processes, you should set a lower value for *number*.

When configuring this memory limit, also note that a certain amount of RP memory is reserved for Layer 3 and Layer 4 ACL data. The amount of memory reserved for ACL data can be viewed using the **show access-list compiled** command, and can be changed using the **access-list compiled ipv4 limit memory** command.

Note that the **no** form of this command removes all memory limits for ACL processing, thereby allowing as much memory as is needed for Layer 2 ACL processing in the RP path.

To restore a default configuration of this command, which is 128 MB, enter the **default** form of this command.

Examples

The following example reserves 100 MB of memory for Layer 2 ACL processing in the RP path:

```
access-list compiled data-link limit memory 100
```

The following example allows Layer 2 ACL processing to use as much memory as is needed for Layer 2 ACL processing:

```
no access-list compiled data-link limit memory
```

The following example restores the default amount of memory reserved for Layer 2 ACL processing in the RP path:

```
default access-list compiled data-link limit memory
```

Related Commands

Command	Description
access-list compiled ipv4 limit memory	Configures limits on the amount of memory used for Turbo ACL processing of Layer 3 and Layer 4 traffic.
show access-list compiled	Displays the status and condition of the Turbo ACL tables associated with each access list.

access-list compiled ipv4 limit memory

To change the amount of memory reserved for Turbo ACL processing for Layer 3 and Layer 4 traffic in the Route Processor path for a Cisco 7304 router using a network services engine (NSE), use the **access-list compiled ipv4 limit memory** command in global configuration mode. To place no restrictions on the amount of memory reserved for Turbo ACL processing for Layer 3 and Layer 4 traffic in the Route Processor path for a Cisco 7304 router using an NSE, use the **no** form of this command. To restore the default amount of memory reserved for Turbo ACL processing for Layer 3 and Layer 4 traffic in the Route Processor path for a Cisco 7304 router using an NSE, use the **default** form of this command.

access-list compiled ipv4 limit memory *number*

no access-list compiled ipv4 limit memory

default access-list compiled ipv4 limit memory

Syntax Description

number	A number between 8 and 4095 that specifies the memory limit in megabytes.

Command Default

On an NSE-150, the default for *number* is always 256.

On an NSE-100, the default for *number* is determined by the amount of SDRAM on the NSE-100. If the NSE-100 has 512 MB of DRAM, the default for *number* is 256. If the NSE-100 has less than 512 MB DRAM, the default for *number* is 128.

Command Modes

Global configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced.

Usage Guidelines

The **show access-list compiled** command output provides information useful in helping to consider the exact memory limit to configure. The following sections of the **show access-list compiled** output, which are found in the "Compiled ACL statistics for IPv4:" section of the output, are especially useful:

- The "mem limits" output shows the number of times a compile has occurred and the ACL has reached its configured limit.
- The "Mb limit" output shows the current memory limit setting.
- The "Mb max memory" output shows the maximum amount of memory the current ACL configuration could actually consume under maximum usage conditions.

Note that there is a direct trade-off between memory used for ACL processing in the RP path and the memory used for other RP processes. Memory reserved for ACL processing cannot be used for other RP processes, and vice versa. If you need more memory for ACL processing, you should set a higher value for *number*. If you need more memory for other RP processes, you should set a lower value for *number*.

When configuring this memory limit, also note that a certain amount of RP memory is reserved for Layer 2 ACL data. The amount of memory reserved for ACL data can be viewed using the **show access-list compiled** command, and can be changed using the **access-list compiled data-link limit memory** command.

Note that the **no** form of this command removes all memory limits for ACL processing, thereby allowing as much memory as is needed for Layer 3 and Layer 4 ACL processing in the RP path.

To restore a default configuration of this command, enter the **default** form of this command.

Examples

The following example reserves 100 MB of memory for Layer 3 and Layer 4 ACL processing in the RP path:

```
access-list compiled ipv4 limit memory 100
```

The following example allows Layer 3 and Layer 4 ACL processing to use as much memory as is needed for Layer 3 and Layer 4 ACL processing:

```
no access-list compiled ipv4 limit memory
```

The following example restores the default amount of memory reserved for Layer 3 and Layer 4 ACL processing in the RP path:

```
default access-list compiled ipv4 limit memory
```

Related Commands

Command	Description
access-list compiled data-link limit memory	Configures memory limits on the amount of memory reserved for Turbo ACL processing of Layer 2 traffic.
show access-list compiled	Displays the status and condition of the Turbo ACL tables associated with each access list

access-list dynamic-extend

To allow the absolute timer of the dynamic access control list (ACL) to be extended an additional six minutes, use the **access-list dynamic-extend** command in global configuration mode. To disable this functionality, use the **no** form of this command.

access-list dynamic-extend

no access-list dynamic-extend

Syntax Description

This command has no arguments or keywords.

Defaults

6 minutes

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When you try to create a Telnet session to the router to re-authenticate yourself by using the lock-and-key function, use the **access-list dynamic-extend** command to extend the absolute timer of the dynamic ACL by six minutes.

The router must already be configured with the lock-and-key feature, and you must configure the extension *before* the ACL expires.

Examples

The following example shows how to extend the absolute timer of the dynamic ACL:

```
! The router is configured with the lock-and-key feature as follows
access-list 132 dynamic tactik timeout 6 permit ip any any
! The absolute timer will extended another six minutes.
access-list dynamic-extend
```

access-list remark

To write a helpful comment (remark) for an entry in a numbered IP access list, use the **access-list remark** command in global configuration mode.To remove the remark, use the **no** form of this command.

access-list *access-list-number* **remark** [*line*]

no access-list *access-list-number* **remark** [*line*]

Syntax Description

access-list-number	Number of an IP access list.
line	(Optional) Comment that describes the access list entry, up to 100 characters long.

Command Default

The access list entries have no remarks.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The remark can be up to 100 characters long; anything longer is truncated.

Examples

The following example shows how to write comments for workstation abc, which is allowed access, and workstation xyz, which is not allowed access:

```
access-list 1 remark Permit only abc workstation comment
access-list 1 permit 192.0.2.0
access-list 1 remark Do not allow xyz workstation comment
access-list 1 deny 192.0.2.13
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
ip access-list	Defines an IP access list by name.
remark	Writes a helpful comment (remark) for an entry in a named IP access list.

access-profile

To apply your per-user authorization attributes to an interface during a PPP session, use the **access-profile** command in privileged EXEC mode.

access-profile [**merge** | **replace**] [**ignore-sanity-checks**]

Syntax Description

merge	(Optional) Removes existing access control lists (ACLs) while retaining other existing authorization attributes for the interface. • However, using this option installs per-user authorization attributes in addition to the existing attributes. (The default form of the command installs only new ACLs.) The per-user authorization attributes come from all attribute-value (AV) pairs defined in the authentication, authorization, and accounting (AAA) per-user configuration (the user's authorization profile).
replace	(Optional) Removes existing ACLs and all other existing authorization attributes for the interface. • A complete new authorization configuration is then installed, using all AV pairs defined in the AAA per-user configuration. • This option is not normally recommended because it initially deletes all existing configurations, including static routes. This could be detrimental if the new user profile does not reinstall appropriate static routes and other critical information.
ignore-sanity-checks	(Optional) Enables you to use any AV pairs, whether or not they are valid.

Command Default

By default this command removes existing ACLs while retaining other existing authorization attributes for the interface.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRB	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRB.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Usage Guidelines

Remote users can use the **access-profile** command to activate double authentication for a PPP session. Double authentication must be correctly configured for this command to have the desired effect.

You should use this command when remote users establish a PPP link to gain local network access.

The resulting authorization attributes of the interface are a combination of the previous and new configurations.

After you have been authenticated with Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP), you will have limited authorization. To activate double authentication and gain your appropriate user network authorization, you must open a Telnet session to the network access server and execute the **access-profile** command. (This command could also be set up as an autocommand, which would eliminate the need to enter the command manually.)

This command causes all subsequent network authorizations to be made in your username instead of in the remote host's username.

Any changes to the interface caused by this command will stay in effect for as long as the interface stays up. These changes will be removed when the interface goes down. This command does not affect the normal operation of the router or the interface.

The default form of the command, **access-profile**, causes existing ACLs to be unconfigured (removed), and new ACLs to be installed. The new ACLs come from your per-user configuration on an AAA server (such as a TACACS+ server). The ACL replacement constitutes a reauthorization of your network privileges.

The default form of the command can fail if your per-user configuration contains statements other than ACL AV pairs. Any protocols with non-ACL statements will be deconfigured, and no traffic for that protocol can pass over the PPP link.

The **access-profile merge** form of the command causes existing ACLs to be unconfigured and new authorization information (including new ACLs) to be added to the interface. This new authorization information consists of your complete per-user configuration on an AAA server. If any of the new authorization statements conflict with existing statements, the new statements could override the old statements or be ignored, depending on the statement and applicable parser rules. The resulting interface configuration is a combination of the original configuration and the newly installed per-user configuration.

Caution The new user authorization profile (per-user configuration) must *not* contain any invalid mandatory AV pairs, because the command will fail and PPP (containing the invalid pair) will be dropped. If invalid AV pairs are included as *optional* in the user profile, the command will succeed, but the invalid AV pair will be ignored. Invalid AV pair types are listed later in this section.

The **access-profile replace** form of the command causes the entire existing authorization configuration to be removed from the interface, and the complete per-user authorization configuration to be added. This per-user authorization consists of your complete per-user configuration on an AAA server.

Caution Use extreme caution when using the **access-profile replac**e form of the command. It might have detrimental and unexpected results, because this option deletes all authorization configuration information (including static routes) before reinstalling the new authorization configuration.

The following are invalid AV pair types:

- addr
- addr-pool
- frame-relay
- ip-addresses

- source-ip
- tunnel-id
- x25-addresses
- zonelist

Note These AV pair types are invalid only when used with double authentication in the user-specific authorization profile; they cause the **access-profile** command to fail. However, these AV pair types can be appropriate when used in other contexts.

Examples

The following example shows how to apply the per-user authorization attributes to an interface during a PPP session:

```
Router# access-profile merge ignore-sanity-checks
```

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
telnet	Logs in to a host that supports Telnet.

access-restrict

To tie a particular Virtual Private Network (VPN) to a specific interface for access to the Cisco IOS gateway and the services it protects, use the **access-restrict** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove the VPN, use the **no** form of this command.

access-restrict {*interface-name*}

no access-restrict {*interface-name*}

Syntax Description

interface-name	Interface to which the VPN should be tied.

Defaults

The VPN is not tied to a specific interface.

Command Modes

ISAKMP group configuration (config-isakmp-group)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

The Access-Restrict attribute ties a particular VPN group to a specific interface for access to the Cisco IOS gateway and the services it provides.

It may be a requirement that particular customers or groups connect to the VPN gateway via a specific interface that uses a particular policy (as applied by the crypto map on that interface). If this specific interface is required, using the **access-restrict** command will result in validation that a VPN connection is connecting only via that interface (and hence, crypto map) to which it is allowed. If a violation is detected, the connection is terminated.

Multiple restricted interfaces may be defined per group. The Access-Restrict attribute is configured on a Cisco IOS router or in the RADIUS profile. This attribute has local (gateway) significance only and is not passed to the client.

You must enable the **crypto isakmp client configuration group** command, which specifies group policy information that has to be defined or changed, before enabling the **access-restrict** command.

Note

- The Access-Restrict attribute can be applied only by a RADIUS user.
- The attribute can be applied on a per-user basis after the user has been authenticated.
- The attribute can override any similar group attributes.

- User-based attributes are available only if RADIUS is used as the database.The attribute can override any similar group attributes.
- The Access-Restrict attribute is not required if ISAKMP profiles are implemented. ISAKMP profiles with specific policies per VPN group (as defined via the **match identity group** command, which is a subcommand of the **crypto isakmp profile** command), will achieve the same result.

An example of an attribute-value (AV) pair for the Access-Restrict attribute is as follows:

```
ipsec:access-restrict=<interface-name>
```

Examples

The following example shows that the VPN is tied to “ethernet 0”:

```
crypto isakmp client configuration group cisco
 access-restrict ethernet 0
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.

access-template

To manually place a temporary access list entry on a router to which you are connected, use the **access-template** command in privileged EXEC mode.

access-template {*access-list-number* | *name*} *template-name* {*source-address source-wildcard-bit* | **any** | **host** {*hostname* | *source-address*}} {*destination-address dest-wildcard-bit* | **any** | **host** {*hostname* | *destination-address*}} [**timeout** *minutes*]

Syntax Description

access-list-number	Number of the dynamic access list. The ranges are from 100 to 199 and from 2000 to 2699.
name	Name of an IP access list. • The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.
template-name	Name of a dynamic access list.
source-address	Source address in a dynamic access list. • All other attributes are inherited from the original access-list entry.
source-wildcard-bit	Source wildcard bits.
any	Specifies any source hostname.
host	Specifies a specific source host.
hostname	Name of the host.
destination-address	Destination address in a dynamic access list. • All other attributes are inherited from the original access-list entry.
dest-wildcard-bit	Destination wildcard bits.
timeout *minutes*	(Optional) Specifies a maximum time limit, in minutes for each entry within this dynamic list. The range is from 1 to 9999. • This is an absolute time, from creation, that an entry can reside in the list. The default is an infinite time limit and allows an entry to remain permanently.

Command Default

Temporary access lists are not placed on the router.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can use the **access-template** to enable the lock-and-key access feature.

You must always define either an idle timeout (with the **timeout** keyword in this command) or an absolute timeout (with the **timeout** keyword in the **access-list** command). Otherwise, the dynamic access list will remain, even after the user has terminated the session.

Examples

The following example shows how to enable IP access on incoming packets in which the source address is 172.29.1.129 and the destination address is 192.168.52.12. All other source and destination pairs are discarded.

```
Router> enable
Router# access-template 101 payroll host 172.29.1.129 host 192.168.52.12 timeout 2
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
autocommand	Configures the Cisco IOS software to automatically execute a command when a user connects to a particular line.
clear access-template	Clears a temporary access list entry from a dynamic access list manually.
show ip accounting	Displays the active accounting or checkpointed database or displays access list violations.

accounting

To enable authentication, authorization, and accounting (AAA) accounting services to a specific line or group of lines, use the **accounting** command in line configuration mode. To disable AAA accounting services, use the **no** form of this command.

accounting {**arap** | **commands** *level* | **connection** | **exec**} [**default** | *list-name*]

no accounting {**arap** | **commands** *level* | **connection** | **exec**} [**default** | *list-name*]

Syntax Description

arap	Enables accounting on lines configured for AppleTalk Remote Access Protocol (ARAP).
commands *level*	Enables accounting on the selected lines for all commands at the specified privilege level. Valid privilege level entries are 0 through 15.
connection	Enables both CHAP and PAP, and performs PAP authentication before CHAP.
exec	Enables accounting for all system-level events not associated with users, such as reloads on the selected lines.
default	(Optional) The name of the default method list, created with the **aaa accounting** command.
list-name	(Optional) Specifies the name of a list of accounting methods to use. If no list name is specified, the system uses the default. The list is created with the **aaa accounting** command.

Defaults

Accounting is disabled.

Command Modes

Line configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

After you enable the **aaa accounting** command and define a named accounting method list (or use the default method list) for a particular type of accounting, you must apply the defined lists to the appropriate lines for accounting services to take place. Use the **accounting** command to apply the specified method lists (or if none is specified, the default method list) to the selected line or group of lines.

Examples

The following example enables command accounting services (for level 15) using the accounting method list named charlie on line 10:

```
line 10
 accounting commands 15 charlie
```

accounting (gatekeeper)

To enable and define the gatekeeper-specific accounting method, use the **accounting** command in gatekeeper configuration mode. To disable gatekeeper-specific accounting, use the **no** form of this command.

accounting {**username h323id** | **vsa**}

no accounting

Syntax Description

username h323id	Enables H323ID in the user name field of accounting record.
vsa	Enables the vendor specific attribute accounting format.

Defaults

Accounting is disabled.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
12.1(5)XM	The **vsa** keyword was added.
12.2(2)T	The **vsa** keyword was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850 universal gateway.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.3(9)T	This **username h323id** keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To collect basic start-stop connection accounting data, the gatekeeper must be configured to support gatekeeper-specific H.323 accounting functionality. The **accounting** command enables you to send accounting data to the RADIUS server via IETF RADIUS or VSA attributes.

Specify a RADIUS server before using the **accounting** command.

There are three different methods of accounting. The H.323 method sends the call detail record (CDR) to the RADIUS server, the syslog method uses the system logging facility to record the CDRs, and the VSA method collects VSAs.

Examples

The following example enables the gateway to report user activity to the RADIUS server in the form of connection accounting records:

```
aaa accounting connection start-stop group radius
gatekeeper
 accounting
```

The following example shows how to enable VSA accounting:

```
aaa accounting connection start-stop group radius
gatekeeper
 accounting exec vsa
```

The following example configures H.323 accounting using IETF RADIUS attributes:

```
Router(config-gk)# accounting username h323id
```

The following example configures H.323 accounting using VSA RADIUS attributes:

```
Router(config-gk)# accounting vsa
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
gatekeeper	Enters gatekeeper configuration mode.

accounting (line)

To enable authentication, authorization, and accounting (AAA) accounting services to a specific line or group of lines, use the **accounting** command in line configuration mode. To disable AAA accounting services, use the **no** form of this command.

accounting {**arap** | **commands** *level* | **connection** | **exec**} [**default** | *list-name*]

no accounting {**arap** | **commands** *level* | **connection** | **exec**} [**default** | *list-name*]

Syntax Description

arap	Enables accounting on lines configured for AppleTalk Remote Access Protocol (ARAP).
commands *level*	Enables accounting on the selected lines for all commands at the specified privilege level. Valid privilege level entries are 0 through 15.
connection	Enables both CHAP and PAP, and performs PAP authentication before CHAP.
exec	Enables accounting for all system-level events not associated with users, such as reloads on the selected lines.
default	(Optional) The name of the default method list, created with the **aaa accounting** command.
list-name	(Optional) Specifies the name of a list of accounting methods to use. If no list name is specified, the system uses the default. The list is created with the **aaa accounting** command.

Defaults

Accounting is disabled.

Command Modes

Line configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

After you enable the **aaa accounting** command and define a named accounting method list (or use the default method list) for a particular type of accounting, you must apply the defined lists to the appropriate lines for accounting services to take place. Use the **accounting** command to apply the specified method lists (or if none is specified, the default method list) to the selected line or group of lines.

Examples

The following example enables command accounting services (for level 15) using the accounting method list named charlie on line 10:

```
line 10
 accounting commands 15 charlie
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.

accounting (server-group)

To specify RADIUS accounting filters for attributes that are to be sent to the RADIUS server in accounting requests, use the **accounting** command in server-group configuration mode. To disable specific RADIUS accounting filters for attributes that are to be sent to the RADIUS server, use the **no** form of this command.

accounting {**accept** *list-name* | **reject** *list-name* | **acknowledge broadcast** | **reply** {**accept** *list-name* | **reject** *list-name*} | **request** {**accept** *list-name* | **reject** *list-name*} | **system host-config**}

no accounting {**accept** *list-name* | **reject** *list-name* | **acknowledge broadcast** | **reply** {**accept** *list-name* | **reject** *list-name*} | **request** {**accept** *list-name* | **reject** *list-name*} | **system host-config**}

Syntax Description

accept	All attributes are rejected except for required attributes and the attributes specified by the *list-name* argument.
reject	All attributes are accepted except for the attributes listed in the specified *list-name* argument.
list-name	The name of a specific configured RADIUS attribute list.
acknowledge	Sends the specified accounting response.
broadcast	Specifies broadcast accounting.
reply	Reply attributes are accepted or rejected as specified by the *list-name* argument.
request	Request attributes are accepted or rejected as specified by the *list-name* argument.
system	Enables system accounting generation.
host-config	Generates system accounting records when private servers are added or deleted.

Command Default

If specific attributes are not accepted or rejected, all attributes will be accepted.

Command Modes

Server-group configuration (config-sg-radius)#

Command History

Release	Modification
12.2(1)DX	This command was introduced.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(13)T	Platform support was added for the Cisco 7401ASR.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	The following new keywords were added: **system** and **host-config**

Usage Guidelines

An accept or reject list (also known as a filter) for RADIUS accounting allows users to send only the accounting attributes their business requires, thereby reducing unnecessary traffic and allowing users to customize their own accounting data.

Only one filter may be used for RADIUS accounting per server group.

Note The listname must be the same as the listname defined in the **radius-server attribute list** command, which is used with the **attribute** (server-group configuration) command to add to an accept or reject list.

Examples

The following example shows how to specify accept list "usage-only" for RADIUS accounting:

```
Router> enable
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa authentication ppp default group radius-sg
Router(config)# aaa authorization network default group radius-sg
Router(config)# aaa group server radius radius-sg
Router(config-sg-radius)# server 10.1.1.1
Router(config-sg-radius)# accounting accept usage-only
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list usage-only
 attribute 1,40,42-43,46
```

The following examples show how Accounting-On records or Accounting-Off records are generated when the **system host-config** keywords are configured using the **accounting** command in server-group configuration mode:

Accounting-On

In this example, Accounting-On records are generated when private server (server-private 10.10.1.1) is added to a server-group.

```
Router> enable
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa group server radius g2
Router#(config-sg-radius)# accounting system host-config
Router#(config-sg-radius)# server-private 10.10.1.1 --> Debugs when adding a private
server.

*May  6 05:23:25.530: RADIUS/ENCODE(00000011):Orig. component type = AAA
*May  6 05:23:25.530: RADIUS(00000011): Config NAS IP: 0.0.0.0
*May  6 05:23:25.530: RADIUS(00000011): sending
*May  6 05:23:25.530: RADIUS/ENCODE: Best Local IP-Address 10.10.55.9 for Radius-Server
10.64.67.15
*May  6 05:23:25.530: RADIUS(00000011): Send Accounting-Request to 10.10.67.15:1646 id
1646/1, len 48
```

```
*May  6 05:23:25.530: RADIUS:  authenticator 9A 10 D2 10 10 10 10 9D - 75 EE D4 AF 5D CC
8F 6A
*May  6 05:23:25.530: RADIUS:  Acct-Session-Id     [44]  10  "00000002"
*May  6 05:23:25.530: RADIUS:  Acct-Status-Type    [40]  6   Accounting-On            [7]
*May  6 05:23:25.530: RADIUS:  NAS-IP-Address      [4]   6   10.10.55.9
*May  6 05:23:25.530: RADIUS:  Acct-Delay-Time     [41]  6   0
*May  6 05:23:25.550: RADIUS: Received from id 1646/10 10.10.67.15:1646,
Accounting-response, len 20
*May  6 05:23:25.550: RADIUS: authenticator 10 A1 10 10 1A 3F E5 C9 - D1 D1 D6 92 4D 0A F9
04
```

Accounting-Off

In this example, Accounting-Off records are generated when private server (server-private 10.10.10.10) is deleted from a server-group.

```
Router> enable
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa group server radius g2
Router#(config-sg-radius)# accounting system host-config
Router#(config-sg-radius)# no server-private 10.10.10.10 --> Debugs when a private server
is deleted.

*May  6 05:23:34.162: RADIUS/ENCODE(00000011):Orig. component type = AAA
*May  6 05:23:34.162: RADIUS(00000011): Config NAS IP: 0.0.0.0
*May  6 05:23:34.162: RADIUS(00000011): sending
*May  6 05:23:34.166: RADIUS/ENCODE: Best Local IP-Address 10.10.55.9 for Radius-Server
10.64.67.15
*May  6 05:23:34.166: RADIUS(00000011): Send Accounting-Request to 10.10.67.15:1646 id
1646/2, len 48
*May  6 05:23:34.166: RADIUS:  authenticator 0A 1E D6 A9 4C 5A 4B 5B - 2A F4 E1 28 3A CF
87 03
*May  6 05:23:34.166: RADIUS:  Acct-Session-Id     [44]  10  "00000002"
*May  6 05:23:34.166: RADIUS:  Acct-Status-Type    [40]  6   Accounting-Off           [8]
*May  6 05:23:34.166: RADIUS:  NAS-IP-Address      [4]   6   10.10.55.9
*May  6 05:23:34.166: RADIUS:  Acct-Delay-Time     [41]  6   0
*May  6 05:23:34.166: RADIUS: Received from id 1646/10 10.10.67.15:1646,
Accounting-response, len 20
*May  6 05:23:34.166: RADIUS:  authenticator 79 ED 10 55 84 5A 08 8D - 74 03 CE 05 12 A5
DE 75
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict network access to the user.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
attribute (server-group configuration)	Adds attributes to an accept or reject list.
authorization (server-group configuration)	Specifies an accept or reject list for attributes that are returned in an Access-Accept packet from the RADIUS server.
radius-server attribute list	Defines an accept or reject list name.

accounting acknowledge broadcast

To define a designated broadcast accounting server group, use the **accounting acknowledge broadcast** command in server group RADIUS configuration mode. To disable the broadcast functionality, use the **no** form of this command.

accounting acknowledge broadcast

no accounting acknowledge broadcast

Syntax Description

This command has no arguments or keywords.

Defaults

Accounting broadcast functionality is disabled for the RADIUS server group.

Command Modes

Server group RADIUS configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example enables accounting broadcast functionality on RADIUS server group abcgroup:

```
Router(config)# aaa group server radius abcgroup
Router(config-sg-radius)# accounting acknowledge broadcast
```

Related Commands

Command	Description
aaa accounting update	Enables periodic interim accounting records to be sent to the accounting server.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
gw-accounting aaa	Enables VoIP gateway accounting through the AAA system.

accounting dhcp source-ip aaa list

To enable Per IP Subscriber DHCP Triggered RADIUS Accounting for billing or security purposes, use the **accounting dhcp source-ip aaa list** command in access interface configuration mode. To disable Per IP Subscriber DHCP Triggered RADIUS Accounting, use the **no** form of this command.

accounting dhcp source-ip aaa list *method-list-name*

no accounting

Syntax Description

method-list-name	Character string used to name at least one of the accounting methods, tried in a given sequence. Valid values are **default** or a named method list as defined by the **aaa accounting** command.

Command Default

This command is disabled by default. If the **accounting dhcp source-ip aaa list** command for RADIUS accounting is issued without a named method list specified, the default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list. If no default method list is defined, then no accounting takes place.

Command Modes

Access interface

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

Enter the **accounting dhcp source-ip aaa list** command to enable accounting. Use the **aaa accounting** command to create a named method list.

Examples

The following example shows how to define a command accounting method list named “default”.

```
accounting dhcp source-ip aaa list default
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
ip dhcp limit lease per interface	Limits the number of leases offered to DHCP clients behind an ATM RBE unnumbered or serial unnumbered interface.

acl (ISAKMP)

To configure split tunneling, use the **acl** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove this command from your configuration and restore the default value, use the **no** form of this command.

acl *number*

no acl *number*

Syntax Description

number	Specifies a group of access control lists (ACLs) that represent protected subnets for split tunneling purposes.

Defaults

Split tunneling is not enabled; all data is sent via the Virtual Private Network (VPN) tunnel.

Command Modes

ISAKMP group configuration (config-isakmp-group)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **acl** command to specify which groups of ACLs represent protected subnets for split tunneling. Split tunneling is the ability to have a secure tunnel to the central site and simultaneous clear text tunnels to the Internet.

You must enable the **crypto isakmp client configuration group** command, which specifies group policy information that has to be defined or changed, before enabling the **acl** command.

Examples

The following example shows how to correctly apply split tunneling for the group name “cisco.” In this example, all traffic sourced from the client and destined to the subnet 192.168.1.0 will be sent via the VPN tunnel.

```
crypto isakmp client configuration group cisco
  key cisco
  dns 10.2.2.2 10.3.2.3
  pool dog
  acl 199
!
access-list 199 permit ip 192.168.1.0 0.0.0.255 any
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies the policy profile of the group that will be defined.

acl (WebVPN)

To define an access control list (ACL) using a Secure Socket Layer Virtual Private Network (SSL VPN) gateway at the Application Layer level and to associate an ACL with a policy group, use the **acl** command in webvpn context configuration and webvpn group policy configuration modes. To remove the ACL definition, use the **no** form of this command.

acl *acl-name*

no acl *acl-name*

Syntax Description

acl-name	Name of the ACL.

Command Default

If a user session has no ACL attributes configured, all application requests are permitted.

Command Modes

Web context configuration
Webvpn group policy configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

The ACL can be defined for an individual user or for a policy group.

A defined ACL can be overridden by an individual user when the user logs on to the gateway (using AAA policy attributes).

Examples

The following example shows that "acl1" has been defined as the ACL and that it has been associated with policy group "default."

```
webvpn context context1
 acl acl1
  permit url "http://www.example.com"
 policy group default
  acl acl1
```

Related Commands

Command	Description
policy group	Configures a policy group and enters group policy configuration mode.
webvpn context	Configures the SSL VPN context and enters webvpn context configuration mode.

action-type

To enable the type of action to be performed on accounting records, use the **action-type** command in accounting method list configuration mode. To disable the action for the accounting records, use the **no** form this command.

action-type {**none** | **start-stop** | **stop-only**}

no action-type {**none** | **start-stop** | **stop-only**}

Cisco 1000 Series Router

action-type {**none** | **start-stop** [**periodic** {**disable** | **interval** *minutes*}] | **stop-only**}

no action-type {**none** | **start-stop** [**periodic** {**disable** | **interval** *minutes*}] | **stop-only**}

Syntax Description

none	Sets the action-type of the accounting records to none.
start-stop	Sets the start and stop action for the accounting records.
stop-only	Sets the stop action for the accounting records when service terminates.
periodic	(Optional) Specifies the periodic accounting action.
disable	Disables periodic accounting action.
interval	Sets the periodic accounting interval.
minutes	Periodic interval, in minutes, for accounting update records.

Command Default

If the periodic interval is not specified, information of all periodic accounting records is displayed.

Command Modes

accounting method list configuration (cfg-acct-mlist)

Command History

Release	Modification
15.0 (1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **action-type** command to enable the type of action to be performed on accounting records.

Examples

The following is sample output from the **action-type** command:

```
Router(config)# aaa accounting network default
Router(cfg-acct-mlist)# action-type start-stop periodic interval 1
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.

activate

To activate fail-close mode so that unencrypted traffic cannot pass through a group member before that member is registered with a key server, use the **activate** command in crypto map fail-close configuration mode. To disable fail-close mode, use the **no** form of this command.

activate

no activate

Syntax Description

This command has no arguments or keywords.

Command Default

Fail-close mode is not activated.

Command Modes

Crypto map fail-close configuration (crypto-map-fail-close)

Command History

Release	Modification
12.4(22)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

The **crypto map** command and **gdoi fail-clos**e keywords must precede this command. However, fail-close mode is not activated until the **activate** command is also configured.

Examples

The following example shows that fail-close mode has been activated, and unencrypted traffic from access list 102 is allowed before the group member is registered:

```
crypto map map1 gdoi fail-close
 match address 102
 activate crypto map map1 10 gdoi
 set group ks1_group
 match address 101
!
access-list 101 deny ip 10.0.1.0 0.0.0.255 10.0.1.0 0.0.0.255
access-list 102 deny tcp any eq telnet any
```

Related Commands

Command	Description
show crypto map gdoi fail-close	Displays information about the status of the fail-close mode.

add (WebVPN)

To add an ACL entry at a specified position, use the **add** command in webvpn acl configuration mode. To remove an entry from the position specified, use the **no** form of this command.

add *position acl-entry*

no add *position acl-entry*

Syntax Description

position	Position in the entry list to which the ACL rule is to be added.
acl-entry	Permit or deny command string.

Command Default

The ACL entry is appended to the end of the entry list.

Command Modes

Webvpn acl configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Examples

The following example shows that the ACL rule should be added to the third position of the ACL list:

```
webvpn context context1
 acl acl1
  add 3 permit url any
```

Related Commands

Command	Description
acl	Defines an ACL using a SSL VPN gateway at the Application Layer level.
wevpn context	Configures the SSL VPN context and enters webvpn context configuration mode.

address

To specify the IP address of the Rivest, Shamir, and Adelman (RSA) public key of the remote peer that you will manually configure in the keyring, use the **address** command in rsa-pubkey configuration mode. To remove the IP address, use the **no** form of this command.

address *ip-address*

no address *ip-address*

Syntax Description

ip-address	IP address of the remote peer.

Defaults

No default behavior or values

Command Modes

Rsa-pubkey configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Before you can use this command, you must enter the **rsa-pubkey** command in the crypto keyring mode.

Examples

The following example specifies the RSA public key of an IP Security (IPSec) peer:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```

Related Commands

Command	Description
crypto keyring	Defines a crypto keyring to be used during IKE authentication.
key-string	Specifies the RSA public key of a remote peer.
rsa-pubkey	Defines the RSA manual key to be used for encryption or signatures during IKE authentication.

address (IKEv2 keyring)

To specify an IPv4 or IPv6 address or the range of the peer in an Internet Key Exchange Version 2 (IKEv2) keyring, use the **address** command in IKEv2 keyring peer configuration mode. To remove the IP address, use the **no** form of this command.

address {*ipv4-address* [*mask*] | *ipv6-address prefix*}

no address

Syntax Description

ipv4-address	IPv4 address of the remote peer.
mask	(Optional) Subnet mask.
ipv6-address	IPv6 address of the remote peer.
prefix	Prefix length

Command Default

The IP address is not specified.

Command Modes

IKEv2 keyring peer configuration (config-ikev2-keyring-peer)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. Support was added for IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to specify the peer's IP address, which is the IKE endpoint address and independent of the identity address.

Examples

The following examples show how to specify the preshared key of an IP Security (IPsec) peer:

```
Router(config)# crypto ikev2 keyring keyring1
Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# address 10.0.0.1 255.255.255.0

Router(config)# crypto ikev2 keyring keyring2
Router(config-ikev2-keyring)# peer peer2
Router(config-ikev2-keyring-peer)# address 2001:DB8:0:ABCD::1/2
```

Related Commands

Command	Description
crypto ikev2 keyring	Defines an IKEv2 keyring.
description (ikev2 keyring)	Describes an IKEv2 peer or a peer group for the IKEv2 keyring.
hostname (ikev2 keyring)	Specifies or modifies the hostname for the network server or peer.
peer	Defines a peer or a peer group for the keyring.
identity (ikev2 keyring)	Identifies the peer with IKEv2 types of identity.
pre-shared-key (ikev2 keyring)	Defines a preshared key for the IKEv2 peer.

address ipv4

To configure the IP address of a Diameter peer, use the **address ipv4** command in Diameter peer configuration submode. To disable the configured address, use the **no** form of this command.

address ipv4 *ip-address*

no address ipv4 *ip-address*

Syntax Description

ip address	The IP address of the host.

Command Default

No IP address is configured.

Command Modes

Diameter peer configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Examples

The following example shows how to configure the IP address of a Diameter peer:

```
Router (config-dia-peer)# address ipv4 192.0.2.0
```

Related Commands

Command	Description
diameter peer	Defines a Diameter peer and enters Diameter peer configuration mode.

address ipv4 (GDOI)

To set the source address, which is used as the source for packets originated by the local key server, use the **address ipv4** command in GDOI local server configuration mode. To remove the source address, use the **no** form of this command.

address ipv4 *ip-address*

no address ipv4 *ip-address*

Syntax Description

ip-address	Source address of the local key server.

Command Default

A source address is not configured.

Command Modes

GDOI local server configuration (config-local-server)

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

When this command is used with unicast rekeys, the address is used as the source of the outgoing rekey message. When this command is used with redundancy, the address is used as the source of the outgoing announcement message. If both unicast rekeying and redundancy are configured, the same address is the source of both types of packets.

If multicast rekeying is configured and the **address ipv4** command is configured, the address (*ip-address)* is the source of the outgoing multicast packet. If multicast is configured but the **address ipv4** command is not configured, the access control list (ACL) specified in the **rekey address ipv4** command identifies the source of the outgoing multicast packet.

Examples

The following example shows the local server IP address is 10.1.1.0:

```
server local
 rekey algorithm aes 192
 rekey address ipv4 121
 rekey lifetime seconds 300
 rekey retransmit 10 number 2
 rekey authentication mypubkey rsa mykeys
 address ipv4 10.1.1.0
 sa ipsec 1
```

Related Commands

Command	Description
rekey address ipv4	Sends a rekey to a destination multicast address.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

addressed-key

To specify which peer's RSA public key you will manually configure, use the **addressed-key** command in public key chain configuration mode.

addressed-key *key-address* [**encryption** | **signature**]

Syntax Description

key-address	Specifies the IP address of the remote peer's RSA keys.
encryption	(Optional) Indicates that the RSA public key to be specified will be an encryption special usage key.
signature	(Optional) Indicates that the RSA public key to be specified will be a signature special usage key.

Defaults

If neither the **encryption** nor **signature** keywords are used, general purpose keys will be specified.

Command Modes

Public key chain configuration. This command invokes public key configuration mode.

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command or the **named-key** command to specify which IP Security peer's RSA public key you will manually configure next.

Follow this command with the **key string** command to specify the key.

If the IPSec remote peer generated general-purpose RSA keys, do not use the **encryption** or **signature** keywords.

If the IPSec remote peer generated special-usage keys, you must manually specify both keys: use this command and the **key-string** command twice and use the **encryption** and **signature** keywords respectively.

Examples

The following example manually specifies the RSA public keys of two IPSec peers. The peer at 10.5.5.1 uses general-purpose keys, and the other peer uses special-usage keys.

```
Router(config)# crypto key pubkey-chain rsa
Router(config-pubkey-chain)# named-key otherpeer.example.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey-key)# key-string
Router(config-pubkey)# 005C300D 06092A86 4886F70D 01010105
Router(config-pubkey)# 00034B00 30480241 00C5E23B 55D6AB22
```

```
Router(config-pubkey)# 04AEF1BA A54028A6 9ACC01C5 129D99E4
Router(config-pubkey)# 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
Router(config-pubkey)# BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
Router(config-pubkey)# D58AD221 B583D7A4 71020301 0001
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(config-pubkey-chain)# addressed-key 10.1.1.2 encryption
Router(config-pubkey-key)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(config-pubkey-chain)# addressed-key 10.1.1.2 signature
Router(config-pubkey-key)# key-string
Router(config-pubkey)# 0738BC7A 2BC3E9F0 679B00FE 53987BCC
Router(config-pubkey)# 01030201 42DD06AF E228D24C 458AD228
Router(config-pubkey)# 58BB5DDD F4836401 2A2D7163 219F882E
Router(config-pubkey)# 64CE69D4 B583748A 241BED0F 6E7F2F16
Router(config-pubkey)# 0DE0986E DF02031F 4B0B0912 F68200C4
Router(config-pubkey)# C625C389 0BFF3321 A2598935 C1B1
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(config-pubkey-chain)# exit
Router(config)#
```

Related Commands

Command	Description
crypto key pubkey-chain rsa	Enters public key configuration mode (to allow you to manually specify the RSA public keys of other devices).
key-string (IKE)	Specifies the RSA public key of a remote peer.
named-key	Specifies which peer RSA public key you will manually configure.
show crypto key pubkey-chain rsa	Displays peer RSA public keys stored on your router.

administrator authentication list

To authenticate an administrative introducer for a Secure Device Provisioning (SDP) transaction, use the **administrator authentication list** command in tti-registrar configuration mode. To disable administrative introducer authentication, use the **no** form of this command.

administrator authentication list *list-name*

no administrator authentication list *list-name*

Syntax Description

list-name	Name of list.

Defaults

All introducers are authenticated as users; their username is used directly to build the device name.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

When you use the **administrator authentication list** command in SDP transactions, the RADIUS or TACACS+ authentication, authorization, and accounting (AAA) server checks for a valid account by looking at the username and password.

The authentication list and the authorization list usually both point to the same AAA list. It is possible that the lists can be on different databases, but it is generally not recommended.

Examples

The following example shows that an administrative authentication list named authen-rad and an administrative authorization list named author-rad have been configured on a RADIUS AAA server; a user authentication list named authen-tac and a user authorization list named author-tac have been configured on a TACACS+ server:

```
Router(config)# crypto provisioning registrar
Router(tti-registrar)# pki-server mycs
Router(tti-registrar)# administrator authentication list authen-rad
Router(tti-registrar)# administrator authorization list author-rad
Router(tti-registrar)# authentication list authen-tac
Router(tti-registrar)# authorization list author-tac
Router(tti-registrar)# template username ftpuser password ftppwd
Router(tti-registrar)# template config ftp://ftp-server/iossnippet.txt
Router(tti-registrar)# end
```

Related Commands

Command	Description
administrator authorization list	Specifies the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS CLI snippet that is sent back to the petitioner for an administrative introducer in an SDP transaction.
authentication list (tti-registrar)	Authenticates an introducer in an SDP transaction.
authorization list (tti-registrar)	Specifies the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS CLI snippet that is sent back to the petitioner for a user introducer in an SDP transaction.

administrator authorization list

To specify the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS command-line interface (CLI) snippet that is sent back to the petitioner for an administrative introducer in a Secure Device Provisioning (SDP) transaction, use the **administrator authorization list** command in tti-registrar configuration mode. To disable the subject name and list of template variables, use the **no** form of this command.

administrator authorization list *list-name*

no administrator authorization list *list-name*

Syntax Description

list-name	Name of list.

Defaults

There is no authorization information requested from the authentication, authorization, and accounting (AAA) server for the administrator.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When you use the **administrator authorization list** command in SDP transactions, the RADIUS or TACACS+ AAA server stores the subject name and template variables. The name and variables are sent back to the petitioner in the Cisco IOS CLI snippets. This list and the authorization list are usually on the same database, but they can be on different AAA databases. (Storing lists on different databases is not recommended.)

When a petitioner makes an introducer request, multiple queries are sent to the AAA list database on the RADIUS or TACACS+ server. The queries search for entries of the following form:

```
user Password <userpassword>
   cisco-avpair="ttti:subjectname=<<DN subjectname>>"
   cisco-avpair="tti:iosconfig#<<value>>"
   cisco-avpair="tti:iosconfig#<<value>>"
   cisco-avpair="tti:iosconfig#=<<value>>"
```

Note The existence of a valid AAA username record is enough to pass the authentication check. The cisco-avpair=tti information is necessary only for the authorization check.

If a subject name were received in the authorization response, the registrar stores it in the enrollment database, and that subject name overrides the subject name that is supplied in the subsequent certificate request (PKCS10) from the petitioner device.

The numbered tti:iosconfig values are expanded into the Cisco IOS snippet that is sent to the petitioner. The configurations replace any numbered ($1 through $9) template variable. Because the default Cisco IOS snippet template does not include the variables $1 through $9, these variables are ignored unless you configure an external Cisco IOS snippet template. To specify an external configuration, use the **template config** command.

Note The template configuration location may include a variable $n, which is expanded to the name that the administrator enters in the additional SDP dialog.

Examples

The following example shows that an administrative authentication list named authen-rad and an administrative authorization list named author-rad have been configured on a RADIUS AAA server; a user authentication list named authen-tac and a user authorization list named author-tac have been configured on a TACACS+ server:

```
Router(config)# crypto provisioning registrar
Router(tti-registrar)# pki-server mycs
Router(tti-registrar)# administrator authentication list authen-rad
Router(tti-registrar)# administrator authorization list author-rad
Router(tti-registrar)# authentication list authen-tac
Router(tti-registrar)# authorization list author-tac
Router(tti-registrar)# template username ftpuser password ftppwd
Router(tti-registrar)# template config ftp://ftp-server/iossnippet.txt
Router(tti-registrar)# end
```

Related Commands

Command	Description
administrator authentication list	Authenticates an administrative introducer for an SDP transaction.
authentication list (tti-registrar)	Authenticates a user introducer for an SDP transaction.
authorization list (tti-registrar)	Specifies the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS CLI snippet that is sent back to the petitioner for a user introducer in an SDP operation.

alert

To enable message logging when events, such as a text-chat, begin, use the **alert** command in the appropriate configuration mode. To change the configured setting or revert to the default setting, use the **no** form of this command.

alert {**on** | **off**}

no alert

Syntax Description

on	Enables message logging for instant messenger application policy events.
off	Disables message logging for instant messenger application policy events.

Command Default

If this command is not configured, the global setting for the **ip inspect alert-off** command will take effect.

Command Modes

cfg-appfw-policy-aim configuration

cfg-appfw-policy-ymsgr configuration

cfg-appfw-policy-msnmsgr configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Examples

The following example shows to enable audit trail messages for all AOL instant messenger traffic:

```
appfw policy-name my-im-policy
 application http
  port-misuse im reset
!
 application im aol
  server deny name login.user1.aol.com
  audit trail on
  alert on
```

Related Commands

Command	Description
ip inspect alert-off	Disables Cisco IOS firewall alert messages.

alert (zone-based policy)

To turn on and off Cisco IOS stateful packet inspection alert messages that are displayed on the console, use the **alert** command in parameter-map type inspect configuration mode or URL parameter-map configuration mode. To change the configured setting or revert to the default setting, use the **no** form of this command.

alert {**on** | **off**}

no alert {**on** | **off**}

Syntax Description

on	Alert messages are generated.
off	Alert messages are not generated.

Command Default

Alert messages are not issued.

Command Modes

Parameter-map type inspect configuration
URL parameter-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use the **alert** subcommand when you are creating a parameter map.

When you are configuring an inspect type parameter map, you can enter the **alert** subcommand after you enter the **parameter-map type inspect** command.

When you are creating or modifying a URL parameter map, you can enter the **alert** subcommand after you enter the **parameter-map type urlfilter** command.

For more detailed information about creating a parameter map, see the **parameter-map type inspect** or **parameter-map type urlfilter** command.

Examples

The following example shows a sample inspect parameter map with the Cisco IOS stateful packet inspection alert messages enabled:

```
parameter-map type inspect insp-params
 alert on
```

Related Commands

Command	Description
ip inspect alert-off	Disables Cisco IOS firewall alert messages.
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
parameter-map type urlfilter	Creates or modifies a parameter map for URL filtering parameters.

alert-severity

To change the alert severity rating for a given signature or signature category, use the **alert-severity** command in signature-definition-action (config-sigdef-action) or IPS-category-action (config-ips-category-action) configuration mode. To return to the default action, use the **no** form of this command.

alert-severity {**high** | **medium** | **low** | **informational**}

no alert-severity

Syntax Description

high | **medium** | **low** | **informational**	Alert severity action for a given signature or signature category.

Command Default

No default behavior or values

Command Modes

Signature-definition-action configuration (config-sigdef-action)
IPS-category-action configuration (config-ips-category-action)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Before issuing the **alert-severity** command, you must specify either a signature via the **signature** command or a signature category (such as attack-type) via the **category** command.

Examples

The following example shows how to set the alert severity value to low for signature 5760:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ips signature-definition
Router(config-sigdef)# signature 5726 0
Router(config-sigdef-sig)# alert-severity low
Router(config-sigdef)#^ZDo you want to accept these changes? [confirm]
Router#
*Nov 9 21:50:55.847: %IPS-6-ENGINE_BUILDING: multi-string - 3 signatures - 12 of 11
engines
*Nov 9 21:50:55.859: %IPS-6-ENGINE_READY: multi-string - build time 12 ms - packets for
this engine will be scanned
*Nov 9 21:50:55.859: %SYS-5-CONFIG_I: Configured from console by cisco on console
```

Related Commands

Command	Description
category	Specifies a signature category that is to be used for multiple signature actions or conditions.
signature	Specifies a signature for which the CLI user tunings will be changed.

algorithm

To specify the algorithm to be used for decrypting the filters, use the **algorithm** command in FPM match encryption filter configuration mode.

algorithm *algorithm*

Syntax Description

algorithm	The algorithm to be used for decrypting. Currently, aes256cbc is the only algorithm supported.

Command Default

No algorithm is specified.

Command Modes

FPM match encryption filter configuration (c-map-match-enc-config)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

If you have access to an encrypted traffic classification definition file (eTCDF) or if you know valid values to configure encrypted Flexible Packet Matching (FPM) filters, you can configure the same eTCDF through the command-line interface instead of using the preferred method of loading the eTCDF on the router. You must create a class map of type access-control using the **class-map type** command, and use the **match encrypted** command to configure the match criteria for the class map on the basis of encrypted FPM filters and enter FPM match encryption filter configuration mode. You can then use the appropriate commands to specify the algorithm, cipher key, cipher value, filter hash, filter ID, and filter version. You can copy the values from the eTCDF by opening the eTCDF in any text editor.

Use the **algorithm** command to specify the algorithm used for decrypting the filters.

Examples

The following example shows how to specify the algorithm for decrypting the filter:

```
Router(config)# class-map type access-control match-all c1
Router(config-cmap)# match encrypted
Router(c-map-match-enc-config)# algorithm aes256cbc
Router(c-map-match-enc-config)#
```

Related Commands

Command	Description
class-map type	Creates a class map to be used for matching packets to a specified class.
match encrypted	Configures the match criteria for a class map on the basis of encrypted FPM filters and enters FPM match encryption filter configuration mode.

all (profile map configuration)

To specify that all authentication and authorization requests be cached, use the **all** command in profile map configuration mode. To disable the caching of all requests, use the **no** form of this command.

all [**no-auth**]

no all

Syntax Description

no-auth	(Optional) Specifies that authentication is bypassed for this user.

Command Default

No requests are cached.

Command Modes

Profile map configuration (config-profile-map)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **all** command to cache all authentication and authorization requests.

Use the **all** command for specific service authorization requests, but it should be avoided when dealing with authentication requests.

Examples

The following example caches all authorization requests in the localusers cache profile group. No authentication is performed for these users because the **no-auth** keyword is used.

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa cache profile localusers
Router(config-profile-map)# all no-auth
```

Related Commands

Command	Description
profile	Defines or modifies an individual authentication and authorization cache profile based on an exact username match.
regexp	Creates an entry in a cache profile group that allows authentication and authorization matches based on a regular expression.

allow-mode

To turn the default mode of the filtering algorithm on or off, use the **allow-mode** command in URL parameter-map configuration mode. To disable this feature, use the **no** form of this command.

allow-mode {**on** | **off**}

no allow-mode {**on** | **off**}

Syntax Description

on	Turns on the default mode of the filtering algorithm. The default is on.
off	Turns off the default mode of the filtering algorithm.

Command Default

The filtering algorithm is turned on.

Command Modes

URL parameter-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

When you are creating or modifying a URL parameter map, you can enter the **allow-mode** subcommand after you enter the **parameter-map type urlfilter** command.

For more detailed information about creating a parameter map, see the **parameter-map type urlfilter** command.

Examples

The following example turns on the filtering algorithm:

```
parameter-map type urlfilter eng-filter-profile
 allow-mode on
```

Related Commands

Command	Description
parameter-map type urlfilter	Creates or modifies a parameter map for URL filtering parameters.

appfw policy-name

To define an application firewall policy and put the router in application firewall policy configuration mode, use the **appfw policy-name** command in global configuration mode. To remove a policy from the router configuration, use the **no** form of this command.

appfw policy-name *policy-name*

no appfw policy-name *policy-name*

Syntax Description

policy-name	Name of application policy.

Defaults

If this command is not issued, an application firewall policy cannot be created.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command puts the router in application firewall policy (appfw-policy-*protocol)* configuration mode, which allows you to begin defining the application firewall policy that will later be applied to the Cisco IOS Firewall via the **ip inspect name** command.

What Is an Application Firewall Policy?

The application firewall uses static signatures to detect security violations. A static signature is a collection of parameters that specifies which protocol conditions must be met before an action is taken. (For example, a signature may specify that an HTTP data stream containing the POST method must reset the connection.) These protocol conditions and reactions are defined by the end user via a command-line interface (CLI) to form an application firewall policy (also known as a security policy).

Examples

The following example shows how to define the HTTP application firewall policy “mypolicy.” This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule “firewall,” which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
```

```
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

Related Commands

Command	Description
application	Puts the router in appfw-policy-*protocol* configuration mode and begin configuring inspection parameters for a given protocol.
ip inspect name	Defines a set of inspection rules.

appl (webvpn)

To configure an application to access a smart tunnel, use the **appl** command in WebVPN smart tunnel configuration mode. To disable an application from accessing the smart tunnel, use the **no** form of this command.

appl *display-name appl-name* **windows**

no appl *display-name appl-name* **windows**

Syntax Description

display-name	Name of the application to be displayed in the smart tunnel application access list on the web browser.
appl-name	Application name or path.
windows	Specifies the Windows platform.

Command Default

No applications have access to a smart tunnel.

Command Modes

WebVPN smart tunnel configuration mode (config-webvpn-smart-tunnel)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

You must configure the correct path and application name to allow the smart tunnel to provide access to applications.

Examples

The following example shows how to configure applications to access the smart tunnel:

```
Router(config)# webvpn context sslgw
Router(config-webvpn-context)# smart-tunnel list st1
Router(config-webvpn-smart-tunnel)# appl ie ieexplore.exe windows
Router(config-webvpn-smart-tunnel)# appl telnet telnet.exe windows
```

Related Commands

Command	Description
smart-tunnel list	Configures the smart tunnel list and enables it within a policy group.
webvpn context	Configures the SSL VPN context.

application (application firewall policy)

To put the router in appfw-policy-*protocol* configuration mode and begin configuring inspection parameters for a given protocol, use the **application** command in application firewall policy configuration mode. To remove protocol-specific rules, use the **no** form of this command.

application *protocol*

no application *protocol*

Syntax Description

protocol	Protocol-specific traffic will be inspected. One of the following protocols (keywords) can be specified: • **http** (HTTP traffic will be inspected.) • **im** {**aol** | **yahoo** | **msn**} (Traffic for the specified instant messenger application will be inspected.)

Command Default

You cannot set up protocol-specific inspection parameters.

Command Modes

cfg-appfw-policy-aim configuration

cfg-appfw-policy-ymsgr configuration

cfg-appfw-policy-msnmsgr configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	The **im**, **aol**, **yahoo**, and **msn** keywords were introduced to support instant message traffic detection and prohibition.

Examples

This command puts the router in appfw-policy-*protocol* configuration mode, where "*protocol*" is dependent upon the specified protocol.

HTTP-Specific Inspection Commands

After you issue the **application http** command and enter the appfw-policy-http configuration mode, begin configuring inspection parameters for HTTP traffic by issuing any of the following commands:

- **audit-trail**
- **content-length**
- **content-type-verification**
- **max-header-length**
- **max-uri-length**
- **port-misuse**

- **request-method**
- **strict-http**
- **timeout**
- **transfer-encoding**

Instant Messenger-Specific Inspection Commands

After you issue the **application im** command and specify an instant messenger application (AOL, Yahoo, or MSN), you can begin configuring inspection parameters for IM traffic by issuing any of the following commands:

- **alert**
- **audit trail**
- **server**
- **service**
- **timeout**

Examples

The following example shows how to define the HTTP application firewall policy "mypolicy." This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule "firewall," which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

The following example shows to configure application policy "my-im-policy," which allows text-chat for Yahoo! instant messenger users and blocks instant messenger traffic for all other users:

```
appfw policy-name my-im-policy
 application http
  port-misuse im reset
!
 application im yahoo
  server permit name scs.msg.yahoo.com
  server permit name scsa.msg.yahoo.com
```

```
  server permit name scsb.msg.yahoo.com
  server permit name scsc.msg.yahoo.com
  service text-chat action allow
  service default action reset
!
 application im aol
  server deny name login.user1.aol.com
!
 application im msn
  server deny name messenger.hotmail.com
!
ip inspect name test appfw my-im-policy

interface FastEthernet0/0
 description Inside interface
 ip inspect test in
```

Related Commands

Command	Description
appfw policy-name	Defines an application firewall policy and puts the router in application firewall policy configuration mode.

application redundancy

To enter redundancy application configuration mode, use the **application redundancy** command in redundancy configuration mode.

application redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Redundancy configuration (config-red)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following example shows how to enter redundancy application configuration mode:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)#
```

Related Commands

Command	Description
group(firewall)	Enters redundancy application group configuration mode.

arap authentication

To enable authentication, authorization, and accounting (AAA) authentication for AppleTalk Remote Access Protocol (ARAP) on a line, use the **arap authentication** command in line configuration mode. To disable authentication for an ARAP line, use the **no** form of this command.

arap authentication {**default** | *list-name*} [**one-time**]

no arap authentication {**default** | *list-name*}

Caution If you use a *list-name* value that was not configured with the **aaa authentication arap** command, ARAP will be disabled on this line.

Syntax Description

default	Default list created with the **aaa authentication arap** command.
list-name	Indicated list created with the **aaa authentication arap** command.
one-time	(Optional) Accepts the username and password in the username field.

Defaults

ARAP authentication uses the default set with **aaa authentication arap** command. If no default is set, the local user database is checked.

Command Modes

Line configuration

Command History

Release	Modification
10.3	This command was introduced.
11.0	The **one-time** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is a per-line command that specifies the name of a list of AAA authentication methods to try at login. If no list is specified, the default list is used (whether or not it is specified in the command line). You create defaults and lists with the **aaa authentication arap** command. Entering the **no** version of **arap authentication** has the same effect as entering the command with the **default** keyword. Before issuing this command, create a list of authentication processes by using the **aaa authentication arap** global configuration command.

Examples

The following example specifies that the TACACS+ authentication list called *MIS-access* is used on ARAP line 7:

```
line 7
 arap authentication MIS-access
```

Related Commands

Command	Description
aaa authentication arap	Enables an AAA authentication method for ARAP using TACACS+.

ase collector

Note Effective with Cisco IOS Release 12.4(24), the **ase collector** command is not available in Cisco IOS software.

To enter the destination IP address of the Automatic Signature Extraction (ASE) collector server, use the **ase collector** command in global configuration mode. To remove this IP address, use the **no** form of this command.

ase collector *ip-address*

no ase collector *ip-address*

Syntax Description

ip-address	Provides IP connectivity between the ASE sensor and ASE collector.

Command Default

No ASE collector IP address is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(24)	This command was removed.

Usage Guidelines

This command is used on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors.

Examples

The following example shows how to configure an ASE collector IP address:

```
Router(config)# ase collector 10.10.10.3
```

Related Commands

Command	Description
ase enable	Enables the ASE feature on a specified interface.
ase group	Identifies the TIDP group number for the ASE feature.
ase signature extraction	Enables the ASE feature globally on the router.
clear ase signature	Clears ASE signatures that were detected on the router.
debug ase	Provides error, log, messaging, reporting, status, and timer information.
show ase	Shows the ASE run-time status, which includes the TIDP group number.

ase enable

Note Effective with Cisco IOS Release 12.4(24), the **ase enable** command is not available in Cisco IOS software.

To enable the Automatic Signature Extraction (ASE) feature on a specified interface, use the **ase enable** command in interface configuration mode. To disable the ASE feature on a specified interface, use the **no** form of this command.

ase enable

no ase enable

Syntax Description

This command has no arguments or keywords.

Command Default

The ASE feature is disabled on an interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(24)	This command was removed.

Usage Guidelines

This command is used on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors.

Examples

The following example shows how to enable the ASE feature on a specified interface:

```
Router(config-if)# ase enable
```

Related Commands

Command	Description
ase collector	Enters the ASE collector server IP address so that the ASE sensor has IP connectivity to the ASE collector.
ase group	Identifies the TIDP group number for the ASE feature.
ase signature extraction	Enables the ASE feature globally on the router.
clear ase signature	Clears ASE signatures that were detected on the router.
debug ase	Provides error, log, messaging, reporting, status, and timer information.
show ase	Shows the ASE run-time status, which includes the TIDP group number.

ase group

Note Effective with Cisco IOS Release 12.4(24), the **ase group** command is not available in Cisco IOS software.

To identify the Threat Information Distribution Protocol (TIDP) group number used for exchange between the Automatic Signature Extraction (ASE) sensor and ASE collector, use the **ase group** command in global configuration mode. To disable this group number, use the **no** form of this command.

ase group *TIDP-group-number*

no ase group *TIDP-group-number*

Syntax Description

TIDP-group-number	TIDP group number for the ASE feature. The range of group numbers is between 1 and 65535.

Command Default

No TIDP group number is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(24)	This command was removed.

Usage Guidelines

This command is used on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors.

Examples

The following example shows how to configure a TIDP group number for the ASE feature:

```
Router(config)# ase group 10
```

Related Commands

Command	Description
ase collector	Enters the ASE collector server IP address so that the ASE sensor has IP connectivity to the ASE collector.
ase enable	Enables the ASE feature on a specified interface.
ase signature extraction	Enables the ASE feature globally on the router.
clear ase signature	Clears ASE signatures that were detected on the router.

Command	Description
debug ase	Provides error, log, messaging, reporting, status, and timer information.
show ase	Shows the ASE run-time status, which includes the TIDP group number.

ase signature extraction

Note Effective with Cisco IOS Release 12.4(24), the **ase signature extraction** command is not available in Cisco IOS software.

To enable the Automatic Signature Extraction (ASE) feature globally on the router, use the **ase signature extraction** command in global configuration mode. To disable the ASE feature globally on the router, use the **no** form of this command.

ase signature extraction

no ase signature extraction

Syntax Description

This command has no arguments or keywords.

Command Default

The ASE feature is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(24)	This command was removed.

Usage Guidelines

This command is used on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors.

Examples

The following example shows how to enable the ASE feature globally on the router:

```
Router(config)# ase signature extraction
```

Related Commands

Command	Description
ase collector	Enters the ASE collector server IP address so that the ASE sensor has IP connectivity to the ASE collector.
ase group	Identifies the TIDP group number for the ASE feature.
ase enable	Enables the ASE feature on a specified interface.
clear ase signature	Clears ASE signatures that were detected on the router.
debug ase	Provides error, log, messaging, reporting, status, and timer information.
show ase	Displays the ASE run-time status, which includes the TIDP group number.

attribute (server-group)

To add attributes to an accept or reject list, use the **attribute** command in server-group configuration mode. To remove attributes from the list, use the **no** form of this command.

attribute *number* [*number* [*number*]...]

no attribute *number* [*number* [*number*]...]

Syntax Description

number [*number* [*number*]...]	Attributes to include in an accept or reject list. The value can be a single integer, such as 7, or a range of numbers, such as 56–59. At least one attribute value must be specified.

Defaults

If this command is not enabled, all attributes are sent to the network access server (NAS).

Command Modes

Server-group configuration

Command History

Release	Modification
12.2(1)DX	This command was introduced.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(13)T	Platform support was added for the Cisco 7401 ASR.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Used in conjunction with the **radius-server attribute list** command (which defines the list name), the **attribute** command can be used to add attributes to an accept or reject list (also known as a filter). Filters are used to prevent the network access server (NAS) from receiving and processing unwanted attributes for authorization or accounting.

The **attribute** command can be used multiple times to add attributes to a filter. However, if a required attribute is specified in a reject list, the NAS will override the command and accept the attribute. Required attributes are as follows:

Note The user-password (RADIUS attribute 2) and nas-ip (RADIUS attribute 4) attributes can be filtered together successfully in the access request if they are configured to be filtered. An access request must contain either a user-password or a CHAP password or a state. Also, either a NAS IP address or NAS identifier must be present in a RADIUS accounting request.

- For authorization:
  - 2 (user-password)
  - 6 (Service-Type)
  - 7 (Framed-Protocol)
- For accounting:
  - 4 (NAS-IP-Address)
  - 40 (Acct-Status-Type)
  - 41 (Acct-Delay-Time)
  - 44 (Acct-Session-ID)

Note The user will not receive an error at the point of configuring a reject list for required attributes because the list does not specify a purpose—authorization or accounting. The server will determine whether an attribute is required when it is known what the attribute is to be used for.

Examples

The following example shows how to add attributes 2, 4, 12, 217, 6–10, 13, 64–69, and 218 to the list name "standard":

```
radius-server attribute list standard
    attribute 2,4,12,217,6-10,13
    attribute 64-69,218
```

Related Commands

Command	Description
accounting (server-group configuration)	Specifies an accept or reject list for attributes that are to be sent to the RADIUS server in an accounting request.
authorization (server-group configuration)	Specifies an accept or reject list for attributes that are returned in an Access-Accept packet from the RADIUS server.
radius-server attribute list	Defines an accept or reject list name.

attribute map

To attach an attribute map to a particular Lightweight Directory Access Protocol (LDAP) server, use the **attribute map** command in LDAP server configuration mode. To remove the attribute maps, use the **no** form of this command.

attribute map *map-name*

no attribute map *map-name*

Syntax Description

map-name	Attribute map name.

Command Default

No attribute maps exist for any LDAP servers.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

To use the attribute mapping features correctly, you need to understand the Cisco LDAP attribute names and values as well as the user-defined attribute names and values.

Examples

The following example shows how to attach an attrribute map named attribute att_map_1 in an LDAP server:

```
Router(config)# ldap server server1
Router(config-ldap-server)# attribute map att_map_1
```

Related Commands

Command	Description
ldap attribute-map	Configures a dynamic LDAP attribute map.
map-type	Defines the mapping of a attribute in the LDAP server.
show ldap attribute	Displays information about default LDAP attribute mapping.

attribute nas-port format

To configure services to use specific named methods for different service types, which can be set to use their own respective RADIUS server groups, use the **attribute nas-port format** command in server-group configuration mode. To remove the override, which is to use specific named methods for different service types, use the **no** form of this command.

attribute nas-port format *format-type* [*string*]

no attribute nas-port format *format-type* [*string*]

Syntax Description

format-type	Type of format (see Table 13).
string	(Optional) Pattern of the data format (see Table 14).

Defaults

Default format type is used for all services.

Command Modes

Server-group configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The following format types may be configured.

Table 13 Format Types

a	Format is type, channel, or port.
b	Either interface(16), isdn(16), or async(16).
c	Data format (bits): shelf(2), slot(4), port(5), or channel(5).
d	Data format (bits): slot(4), module(1), port(3), vpi(8), or vci(16).
e	Configurable data format (see Table 14).

The following characters may be used in the string pattern of the data format.

Table 14 Characters Supported by Format-Type e

0	Zero
1	One
f	DS0 shelf
s	DS0 slot

Table 14 Characters Supported by Format-Type e (continued)

a	DS0 adapter
P	DS0 port
i	DS0 subinterface
c	DS0 channel
F	Async shelf
S	Async slot
P	Async port
L	Async line
S	PPPoX slot (includes PPP over ATM [PPPoA], PPP over Ethernet over ATM [PPPoEoA], PPP over Ethernet over Ethernet [PPPoEoE], PPP over Ethernet over VLAN [PPPoEoVLAN], and PPP over Ethernet over Queue in Queue [PPPoEoQinQ]).
A	PPPoX adapter
P	PPPoX port
V	PPPoX VLAN ID
I	PPPoX virtual path identifier (VPI)
C	PPPoX virtual channel indicator (VCI)
U	Session ID

Examples

The following example shows that a leased-line PPP client has chosen to send no RADIUS Attribute 5 while the default is set for format d:

```
interface Serial2/0
 no ip address
 encapsulation ppp
 ppp accounting SerialAccounting
 ppp authentication pap

aaa accounting network default start-stop group radius
aaa accounting network SerialAccounting start-stop group group1

aaa group server radius group1
 server 10.101.159.172 auth-port 1645 acct-port 1646
 attribute nas-port none

radius-server host 10.101.159.172 auth-port 1645 acct-port 1646
radius-server attribute nas-port format d
```

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
ip radius source-interface	Forces RADIUS to use the IP addressing of a specified interface for all outgoing RADIUS packets.
radius-server host	Specifies a RADIUS server host.

attribute type

To define an attribute type that is to be added to an attribute list locally on a router, use the **attribute type** command in global configuration mode. To remove the attribute type from the list, use the **no** form of this command.

attribute type *name value* [**service** *service*] [**protocol** *protocol*] [*tag*]

no attribute type *name value* [**service** *service*] [**protocol** *protocol*] [*tag*]

Syntax Description

name	The Cisco IOS authentication, authorization, and accounting (AAA) internal name of the IETF RADIUS attribute to be added to the attribute list. For a list of supported attributes, use the CLI help option (**?**) on your platform.
value	A string, binary, or IPv4 address value. This is the RADIUS attribute that is being defined in Cisco IOS AAA format. A string added to the attribute value must be inside quotation marks. For example, if the value is "interface-config" and the string is "ip unnumbered FastEthernet0," you would write interface-config "ip unnumbered FastEthernet0".
service *service*	(Optional) Specifies the Access method, which is typically PPP.
protocol *protocol*	(Optional) Specifies the type of protocol, which can be ATM, IP, or virtual private dialup network (VPDN).
tag	(Optional) A means of grouping attributes that refer to the same VPDN tunnel.

Command Default

An attribute type is not added to the attribute list.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(55)SE	This command was modified in Cisco IOS Release 12.2(55)SE. The following options were added for the *service* argument: **ap-lsc-join** , **ap-mic-join**, **ap-ssc-join**, **lbs-mic-join**, and **lbs-ssc-join**.

Usage Guidelines

Attributes are added to the attribute list each time a new attribute type is defined. Attributes are not validated at configuration. The AAA subsystem "knows" only the format that is expected by the services when the service defines a given attribute inside a definition file. However, it cannot validate the attribute

information itself. This validation is done by a service when it first uses the attribute. This validation is applicable to both RADIUS and TACACS+ AAA servers. Thus, if you are not familiar in configuring a AAA server, Cisco recommends that you test your attribute list on a test device with the service that will be using the list before configuring and using it in a production environment.

Examples

The following example shows that the attribute list named "TEST" is to be added to the subscriber profile "example.com." The attribute TEST includes the attribute types interface-config "ip unnumbered FastEthernet0" and interface-config "ip vrf forwarding vrf1."

```
aaa authentication ppp template1 local
aaa authorization network template1 local
!
aaa attribute list TEST
   attribute type interface-config "ip unnumbered FastEthernet0" service ppp protocol lcp
   attribute type interface-config "ip vrf forwarding vrf1" service ppp protocol lcp
!
ip vrf blue
 description vrf vrf1 template1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
subscriber authorization enable
!
subscriber profile example.com
 service local
 aaa attribute list TEST
!
bba-group pppoe grp1
 virtual-template 1
 service profile example.com
!
interface Virtual-Template1
 no ip address
 no snmp trap link-status
 no peer default ip address
 no keepalive
 ppp authentication pap template1
 ppp authorization template1
!
```

Related Commands

Command	Description
aaa attribute list	Defines a AAA attribute list locally on a router.

audit filesize

To change the size of the audit file, use the **audit filesize** command in global configuration mode. To return the audit file to its default size, use the **no** form of this command.

audit filesize *size*

no audit filesize *size*

Syntax Description

size	Size of the audit file in KB. Valid values range from 32 KB to 128 KB. 32 KB is the default size.

Defaults

The audit file is 32 KB.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)S	This command was introduced.
12.0(27)S	This feature was integrated into Cisco IOS Release 12.0(27)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The audit file is a fixed file size in the disk file system. The audit file contains syslog messages (also referred to as hashes), which monitor changes that have been made to your router. Because the audit file that is stored on the disk is circular, the number of messages that can be stored is dependent on the size of the selected file. Also, the size determines the number of messages that can be stored on the disk before a wrap around occurs.

You should always ensure that the audit file is secure. The audit file should be access protected so that only the audit subsystem can access it.

Note Audit logs are enabled by default and cannot be disabled.

Examples

The following example shows how to change the audit file size to 128 KB:

```
Router(config)# audit filesize 128
```

Related Commands

Command	Description
audit interval	Changes the time interval that is used for calculating hashes.
show audit	Displays contents of the audit file.

audit interval

To change the time interval that is used for calculating hashes, use the **audit interval** command in global configuration mode. To return to the default value, which is 5 minutes, use the **no** form of this command.

audit interval *seconds*

no audit interval *seconds*

Syntax Description

seconds	Time interval, in seconds, between hash calculations. Valid values range from 120 seconds to 3600 seconds. The default value is 300 seconds (5 minutes).

Defaults

300 seconds (5 minutes)

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)S	This command was introduced.
12.0(27)S	This feature was integrated into Cisco IOS Release 12.0(27)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27) SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Hashes are used to monitor changes in your router. A separate hash is maintained for each of the following areas:

- Running version—A hash of the information that is provided in the output of the **show version** command—running version, ROM information, BOOTLDR information, system image file, system and processor information, and configuration register contents.
- Hardware configuration—A hash of platform-specific information that is generally provided in the output of the **show diag** command.
- File system—A hash of the dir information on all of the flash file systems, which includes bootflash and any other flash file systems on the router.
- Running configuration—A hash of the running configuration.
- Startup configuration—A hash of the contents of the files on NVRAM, which includes the startup-config, private-config, underlying-config, and persistent-data files.

By default, the hashes are calculated every 5 minutes to see if any changes (events) have been made to the network. The time interval prevents a large number of hashes from being generated.

Note Audit logs are enabled by default and cannot be disabled.

Examples

The following example shows how to specify hashes to be calculated every 120 seconds (2 minutes):

```
Router(config)# audit interval 120
```

Related Commands

Command	Description
audit filesize	Changes the size of the audit file.
show audit	Displays contents of the audit file.

audit-trail

To enable message logging for established or torn-down connections, use the **audit-trail** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

audit-trail {**on** | **off**}

no audit-trail {**on** | **off**}

Syntax Description

on	Audit trail messages are generated.
off	Audit trail messages are not generated.

Defaults

If this command is not issued, the default value specified via the **ip inspect audit-trail** command will be used.

Command Modes

cfg-appfw-policy-http configuration

cfg-appfw-policy-aim configuration

cfg-appfw-policy-ymsgr configuration

cfg-appfw-policy-msnmsgr configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	Support for the inspection of instant messenger applications was introduced.

Usage Guidelines

The **audit-trail** command will override the **ip inspect audit-trail** global command.

Before you can issue the **audit-trail** command, you must enable protocol inspection via the **application** command, which allows you to specify whether you want to inspect HTTP traffic or instant messenger application traffic. The **application** command puts the router in appfw-policy-*protocol* configuration mode, where "*protocol*" is dependent upon the specified protocol.

Examples

The following example, which shows how to define the HTTP application firewall policy "mypolicy," enables audit trail messages for the given policy. This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule "firewall," which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  audit trail on
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
```

```
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

Related Commands

Command	Description
ip inspect audit-trail	Turns on audit trail messages.

audit-trail (zone)

To turn audit trail messages on or off, use the **audit-trail** command in parameter-map type inspect configuration mode or URL parameter-map configuration mode. To disable this feature, use the **no** form of this command.

audit trail {**on** | **off**}

no audit trail {**on** | **off**}

Syntax Description

on	Audit trail messages will be issued.
off	Audit trail messages will not be issued.

Command Default

There are no audit trail messages.

Command Modes

Parameter-map type inspect configuration
URL parameter-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use the **audit-trail** subcommand when you are creating a parameter map. For each inspected protocol, you can set the audit trail to **on** or **off**.

When you are configuring an inspect type parameter map, you can enter the **audit-trail** subcommand after you enter the **parameter-map type inspect** command.

When you are creating or modifying a URL parameter map, you can enter the **audit-trail** subcommand after you enter the **parameter-map type urlfilter** command.

For more detailed information about creating a parameter map, see the **parameter-map type inspect** or **parameter-map type urlfilter** command.

Examples

The following example generates audit trail messages:

```
parameter-map type inspect insp-params
 audit-trail on
```

Related Commands

Command	Description
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
parameter-map type urlfilter	Creates or modifies a parameter map for URL filtering parameters.

authentication

To configure clear text authentication and MD5 authentication under a redundancy group protocol, use the **authentication** command in redundancy application protocol configuration mode**.** To disable the authentication settings in the redundancy group, use the **no** form of this command.

authentication {**text** *string* | **md5 key-string** [**0** | **7**] *key* | **md5 key-chain** *key-chain-name*}

no authentication {**text** *string* | **md5 key-string** [**0** | **7**] *key* | **md5 key-chain** *key-chain-name*}

Syntax Description

text *string*	Uses clear text authentication.
md5 key-string	Uses MD5 key authentication. The *key* argument can be up to 64 characters in length (at least 16 characters is recommended). Specifying 7 means the key will be encrypted.
0	(Optional) Specifies that the text following immediately is not encrypted.
7	(Optional) Specifies that the text is encrypted using a Cisco-defined encryption algorithm.
md5 key-chain *key-chain-name*	Uses MD5 key-chain authentication.

Command Default

The key is not encrypted.

Command Modes

Redundancy application protocol configuration (config-red-app-prtcl)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following example shows how to configure clear text authentication for a redundancy group:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# protocol 1
Router(config-red-app-prtcl)# authentication text name1
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.

Command	Description
protocol	Defines a protocol instance in a redundancy group.
timers hellotime	Configures timers for hellotime and holdtime messages for a redundancy group.

authentication (IKE policy)

To specify the authentication method within an Internet Key Exchange (IKE) policy, use the **authentication** command in ISAKMP policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the authentication method to the default value, use the **no** form of this command.

authentication {**rsa-sig** | **rsa-encr** | **pre-share** | **ecdsa-sig**}

no authentication

Syntax Description

rsa-sig	Specifies RSA signatures as the authentication method. This method is not supported in IPv6.
rsa-encr	Specifies RSA encrypted nonces as the authentication method. This method is not supported in IPv6.
pre-share	Specifies preshared keys as the authentication method.
ecdsa-sig	Specifies the Elliptic Curve Digital Signature Algorithm (ECDSA) signature (ECDSA-sig) as the authentication method.

Command Default

The RSA signatures authentication method is used.

Command Modes

ISAKMP policy configuration (config-isakmp)

Command History

Release	Modification
11.3 T	This command was introduced.
12.4(4)T	Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(2)T	This command was modified. The **ecdsa-sig** keyword was added.

Usage Guidelines

Use this command to specify the authentication method to be used in an IKE policy.

If you specify RSA signatures, you must configure your peer routers to obtain certificates from a certification authority (CA).

If you specify RSA encrypted nonces, you must ensure that each peer has the other peer's RSA public keys. (See the **crypto key pubkey-chain rsa**, **addressed-key**, **named-key**, **address**, and commands.)

If you specify preshared keys, you must also separately configure these preshared keys. (See the **crypto isakmp identity** and **crypto isakmp key** commands.)

Examples

The following example configures an IKE policy with preshared keys as the authentication method (all other parameters are set to the defaults):

```
Router(config)# crypto isakmp policy 15
Router(config-isakmp)# authentication pre-share
Router(config-isakmp)# exit
```

Related Commands

Command	Description
crypto isakmp key	Configures a preshared authentication key.
crypto isakmp policy	Defines an IKE policy.
crypto key generate rsa (IKE)	Generates RSA key pairs.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
group (IKE policy)	Specifies the Diffie-Hellman group identifier within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
show crypto isakmp policy	Displays the parameters for each IKE policy.

authentication (IKEv2 profile)

To specify the local and remote authentication methods in an Internet Key Exchange Version 2 (IKEv2) profile, use the **authentication** command in IKEv2 profile configuration mode. To delete the authentication method, use the **no** form of this command.

authentication {**local** {**rsa-sig** | **pre-share** | **ecdsa-sig**} | **remote** {**eap** [**query-identity**]| **rsa-sig** | **pre-share** | **ecdsa-sig**}

no authentication {**local** {**rsa-sig** | **pre-share** | **ecdsa-sig**} | **remote** {**eap** | **rsa-sig** | **pre-share** | **ecdsa-sig**}

Syntax Description

local	Specifies the local authentication method.
rsa-sig	Specifies the RSA signature as the authentication method.
pre-share	Specifies the preshared key as the authentication method.
ecdsa-sig	Specifies the Elliptic Curve Digital Signature Algorithm (ECDSA) signature (ECDSA-sig) as the authentication method.
remote	Specifies the remote authentication method.
eap	Specifies Extensible Authentication Protocol (EAP) as the authentication method.
query-identity	(Optional) Queries EAP identity from the peer.

Command Default

The default local and remote authentication method is pre-share.

Command Modes

IKEv2 profile configuration (crypto-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(2)T	This command was modified. The **ecdsa-sig** keyword was added.
15.1(3)T	This command was modified. The **eap** and **query-identity** keywords were added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to specify the local and remote authentication methods in an IKEv2 profile. You can configure only one local authentication method and multiple remote authentication methods. Multiple remote authentication methods are allowed as the profile caters to multiple peers and the authentication method that a peer uses is not known. However, each remote authentication method must be specified in a separate command.

If the RSA signature is configured as the local or remote authentication method, you must specify the PKI trustpoints to obtain the signing and verification certificates using the **pki trustpoint** command.

If a preshared key is configured as the local or remote authentication method, you must separately configure the preshared keys and the keyring using the command **keyring** to specify the local and remote keys.

If the **query-identity** keyword is specified, the EAP identity request is sent when the remote peer indicates the intent to use EAP authentication by skipping Auth payload in the IKE-AUTH request and the local policy allows EAP authentication for remote peer. The remote EAP identity is used in the following scenarios:

- When the EAP identity is used to switch to another IKEv2 profile.
- The remote EAP identity is passed to the RADIUS EAP server as the username for the peer to be authenticated for external EAP.
- The remote EAP identity is used to derive a name for requests using a name mangler.

Examples

The following example shows how to specify an authentication method to an IKEv2 profile:

```
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# match identity remote address 192.168.1.1
Router(config-ikev2-profile)# authentication local pre-share
Router(config-ikev2-profile)# authentication remote pre-share
Router(config-ikev2-profile)# authentication remote rsa-sig
Router(config-ikev2-profile)# identity local email user1@abc.com
Router(config-ikev2-profile)# keyring keyring-1
Router(config-ikev2-profile)# pki trustpoint tp-remote verify
```

In the above example, the profile profile1 specifies pre-share as the local authentication method and pre-share and rsa-sig as the remote authentication methods that use keyring keyring-1 and the trustpoint tp-remote.

The following example shows how to configure an IKEv2 profile for two peers using different authentication methods:

```
Router(config)# crypto ikev2 profile profile2
Router(config-ikev2-profile)# match identity local email user1@abc.com
Router(config-ikev2-profile)# match identity remote email user2@abc.com
Router(config-ikev2-profile)# authentication local pre-share
Router(config-ikev2-profile)# authentication remote pre-share
```

The above profile caters to two peers: user1@abc.com authenticated with pre-share and user2@abc.com authenticated with rsa-signature.

Related Commands

Command	Description
crypto ikev2 keyring	Defines an IKEv2 keyring.
keyring	Specifies the keyring that used with a preshared key authentication method.
pki trustpoint	Specifies the PKI trustpoints used with RSA signature authentication method.
show crypto ikev2 profile	Displays the IKEv2 profile.

authentication bind-first

To configure the sequence of search and bind of an authentication request in the Lightweight Directory Access Protocol (LDAP) server, use the **authentication bind-first** command in LDAP server configuration mode. To remove the search and bind configuration, use the **no** form of this command.

authentication bind-first

no authentication bind-first

Syntax Description

This command has no arguments or keywords.

Command Default

The search operation is performed first and bind operation is performed later.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

In an LDAP deployment, search operation is performed first and bind operation is performed later. This operation is performed because, if the password attribute is returned as part of the search operation, then password verification can be done locally on the LDAP client and there is no need for an extra bind operation. If the password attribute is not returned, a bind operation can be performed later. Another advantage of performing the search operation first and bind operation later is that the distinguished name (DN) received in the search result can be used as the user DN instead of forming a DN by prefixing the username (cn attribute) with base DN.

Examples

The following example shows how to configure the search and bind operations for an authentication request:

```
Router(config)# ldap server server1
Router(config-ldap-server)# authentication bind-first
```

Related Commands

Command	Description
ldap server	Defines an LDAP server and enters LDAP server configuration mode.

authentication command

To specify the HTTP command that is sent to the certification authority (CA) for authentication, use the **authentication command** in ca-profile-enroll configuration mode.

authentication command {*http-command*}

Syntax Description

http-command	Defines the HTTP command. **Note** The *http-command* argument is not the HTTP URL.

Defaults

No default behavior or values

Command Modes

Ca-profile-enroll configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

Use the **authentication command** to send the HTTP request to the CA server for certificate authentication. Before enabling this command, you must use the **authentication url** command.

After enabling this command, you can use the **parameter** command to specify enrollment parameters for your enrollment profile.

Examples

The following example shows how to configure certificate authentication via HTTP for the enrollment profile named “E”:

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial

crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
authentication url	Specifies the URL of the CA server to which to send authentication requests.
crypto ca profile enrollment	Defines an enrollment profile.
parameter	Specifies parameters for an enrollment profile.

authentication command bounce-port ignore

To configure the router to ignore a RADIUS Change of Authorization (CoA) bounce port command, use the **authentication command bounce-port ignore** command in global configuration mode. Use the **no** form of this command to return to the default status.

authentication command bounce-port ignore

no authentication command bounce-port ignore

Syntax Description

This command has no arguments or keywords.

Defaults

The router accepts a RADIUS CoA bounce port command.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)SE	This command was introduced.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

A RADIUS CoA bounce port command sent from a RADIUS server can cause a link flap on an authentication port, which triggers DHCP renegotiation from one or more hosts connected to this port. This incident can occur when there is a VLAN change and the endpoint is a device (such as a printer), that does not have a mechanism to detect a change on this authentication port. The **authentication command bounce-port ignore** command configures the router to ignore the RADIUS CoA bounce port command to prevent a link flap from occuring on any host(s) that are connected to an authentication port.

Examples

This example shows how to configure the router to ignore a CoA bounce port command:

```
Router(config)# aaa new-model
Router(config)# authentication command bounce-port ignore
```

Related Commands

Command	Description
authentication command disable-port ignore	Configures the router to ignore a RADIUS server CoA disable port command.

authentication command disable-port ignore

To allow the router to ignore a RADIUS server Change of Authorization (CoA) disable port command, use the **authentication command disable-port ignore** command in global configuration mode. Use the **no** form of this command to return to the default status.

authentication command disable-port ignore

no authentication command disable-port ignore

Syntax Description

This command has no arguments or keywords.

Defaults

The router accepts a RADIUS CoA disable port command.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)SE	This command was introduced.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

The RADIUS server CoA disable port command administratively shuts down the authentication port that is hosting a session, resulting in session termination. Use the **authentication command disable-port ignore** command to configure the router to ignore the RADIUS server CoA disable port command so that the authentication port and other hosts on this authentication port are not disconnected.

Examples

This example shows how to configure the router to ignore a CoA **disable port** command:

```
Router(config)# aaa new-model
Router(config)# authentication command disable-port ignore
```

Related Commands

Command	Description
authentication command bounce-port ignore	Configures the router to ignore a RADIUS server CoA bounce port command.

authentication compare

To replace a bind request with a compare request for an authentication, use the **authentication compare** command in LDAP server configuration mode. To disable the comparison of bind operations for the authentication requests, use the **no** form of this command.

authentication compare

no authentication compare

Syntax Description

This command has no arguments or keywords.

Command Default

Authentication request is performed with bind request.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Examples

The following example shows how to replace a bind request with a compare request for an authentication:

```
Router(config)# ldap server server1
Router(config-ldap-server)# authentication compare
```

Related Commands

Command	Description
ldap server	Defines an LDAP server and enters LDAP server configuration mode.

authentication control-direction

To set the direction of authentication control on a port, use the **authentication control-direction** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication control-direction {**both** | **in**}

no authentication control-direction

Syntax Description

both	Enables bidirectional control on the port.
in	Enables unidirectional control on the port.

Command Default

The port is set to bidirectional mode.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

The IEEE 802.1x standard is implemented to block traffic between the nonauthenticated clients and network resources. This means that nonauthenticated clients cannot communicate with any device on the network except the authenticator. The reverse is true, except for one circumstance—when the port has been configured as a unidirectional controlled port.

Unidirectional State

The IEEE 802.1x standard defines a unidirectional controlled port, which enables a device on the network to "wake up" a client so that it continues to be reauthenticated. When you use the **authentication control-direction in** command to configure the port as unidirectional, the port changes to the spanning-tree forwarding state, thus allowing a device on the network to wake the client, and force it to reauthenticate.

Bidirectional State

When you use the **authentication control-direction both** command to configure a port as bidirectional, access to the port is controlled in both directions. In this state, the port does not receive or send packets.

Examples

The following example shows how to enable unidirectional control:

```
Switch(config-if)# authentication control-direction in
```

The following examples show how to enable bidirectional control:

```
Switch(config-if)# authentication control-direction both
```

authentication critical recovery delay

To configure the Auth Manager critical recovery delay, use the **authentication critical recovery delay** command in global configuration mode. To remove a previously configured recovery delay, us the **no** form of this command.

authentication critical recovery delay *milliseconds*

no authentication critical recovery delay

Syntax Description

milliseconds	The period of time, in milliseconds, that the Auth Manager waits to reinitialize a critical port when an unavailable RADIUS server becomes available; valid values are from 1 to 10000.

Command Default

The default delay is 1000 milliseconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Examples

The following example shows how to configure the critical recovery delay period to 1500 milliseconds:

```
Switch(config)# authentication critical recovery delay 1500
```

authentication event fail

To specify how the Auth Manager handles authentication failures as a result of unrecognized user credentials, use the **authentication event fail** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication event fail [**retry** *retry-count*] **action** {**authorize vlan** *vlan-id* | **next-method**}

no authentication event fail

Syntax Description

retry *retry-count*	(Optional) Specifies how many times the authentication method is tried after an initial failure.
action	Specifies the action to be taken after an authentication failure as a result of incorrect user credentials.
authorize vlan *vlan-id*	Authorizes a restricted VLAN on a port after a failed authentication attempt.
next-method	Specifies that the next authentication method be invoked after a failed authentication attempt. The order of authentication methods is specified by the **authentication order** command.

Command Default

Authentication is attempted two times after the initial failed attempt.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

Only the dot1x authentication method can signal this type of authentication failure.

Examples

The following example specifies that after three failed authentication attempts the port is assigned to a restricted VLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3
Switch(config-if)# authentication event fail retry 3 action authorize vlan 40
Switch(config-if)# end
```

Related Commands

Command	Description
authentication event no-response action	Specifies the action to be taken when authentication fails due to a nonresponsive host.
authentication order	Specifies the order in which authentication methods are attempted.

authentication event no-response action

To specify how the Auth Manager handles authentication failures as a result of a nonresponsive host, use the **authentication event no-response action** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication event no-response action authorize vlan *vlan-id*

no authentication event no-response

Syntax Description

authorize vlan *vlan-id*	Authorizes a restricted VLAN on a port after a failed authentication attempt.

Command Default

Authentication fails.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

Use the **authentication event no-response action** command to specify how to handle authentication failures as a result of a nonresponsive host.

Examples

The following example specifies that when authentication fails as a result of a non-responsive host, the port is assigned to a VLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3
Switch(config-if)# authentication event no-response action authorize vlan 40
Switch(config-if)# end
```

Related Commands

Command	Description
authentication event fail	Specifies how the Auth Manager handles authentication failures as a result of unrecognized user credentials

authentication event server alive action reinitialize

To reinitialize an authorized Auth Manager session when a previously unreachable authentication, authorization, and accounting (AAA) server becomes available, use the **authentication event server alive action reinitialize** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication event server alive action reinitialize

no authentication event server alive action reinitialize

Syntax Description

This command has no arguments or keywords.

Command Default

The session is not reinitialized.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

Use the **authentication event server alive action reinitialize** command to reinitialize authorized sessions when a previously unreachable AAA server becomes available.

Examples

The following example specifies that authorized sessions are reinitialized when a previously unreachable AAA server becomes available:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3
Switch(config-if)# authentication event server alive action reinitialize
Switch(config-if)# end
```

Related Commands:

Command	Description
authentication event server dead action authorize	Specifies how to handle authorized sessions when the AAA server is unreachable.

authentication event server dead action authorize

To authorize Auth Manager sessions when the authentication, authorization, and accounting (AAA) server becomes unreachable, use the **authentication event server dead action authorize** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication event server dead action authorize vlan *vlan-id*

no authentication event server dead action authorize

Syntax Description

vlan *vlan-id*	Authorizes a restricted VLAN on a port after a failed authentication attempt.

Command Default

No session is authorized.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

Use the **authentication event server dead action authorize** command to authorize sessions even when the AAA server is unavailable.

Examples

The following example specifies that when the AAA server becomes unreachable, the port is assigned to a VLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3
Switch(config-if)# authentication event server dead action authorize vlan 40
Switch(config-if)# end
```

Related Commands

Command	Description
authentication event server alive action reinitialize	Reinitializes an authorized session when a previously unreachable AAA server becomes available.

authentication fallback

To enable a web authentication fallback method, use the **authentication fallback** command in interface configuration mode. To disable web authentication fallback, use the **no** form of this command.

authentication fallback *fallback-profile*

no authentication fallback

Syntax Description

fallback-profile	The name of the fallback profile for web authentication.

Command Default

Web authentication fallback is not enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

Use the **authentication fallback** command to specify the fallback profile for web authentication. Use the **fallback profile** command to specify the details of the profile.

Examples

The following example shows how to specify a fallback profile on a port:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# authentication fallback profile1
Switch(config-if)# end
```

Related Commands

Command	Description
fallback profile	Specifies the profile for web authentication.

authentication host-mode

To allow hosts to gain access to a controlled port, use the **authentication host-mode** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication host-mode {**single-host** | **multi-auth** | **multi-domain** | **multi-host**} [**open**]

no authentication host-mode

Syntax Description

single-host	Specifies that only one client can be authenticated on a port at any given time. A security violation occurs if more than one client is detected.
multi-auth	Specifies that multiple clients can be authenticated on the port at any given time.
multi-domain	Specifies that only one client per domain (DATA or VOICE) can be authenticated at a time.
multi-host	Specifies that after the first client is authenticated, all subsequent clients are allowed access.
open	(Optional) Specifies that the port is open; that is, there are no access restrictions.

Command Default

Access to a port is not allowed.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

Before you use this command, you must use the **authentication port-control** command with the keyword **auto**.

In **multi-host** mode, only one of the attached hosts has to be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (reauthentication fails or an Extensible Authentication Protocol over LAN [EAPOL] logoff message is received), all attached clients are denied access to the network.

Examples

:The following example shows how to enable authentication in multi-host mode:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# authentication port-control auto
Switch(config-if)# authentication host-mode multi-host
```

authentication list (tti-registrar)

To authenticate the introducer in an Secure Device Provisioning (SDP) transaction, use the **authentication list** command in tti-registrar configuration mode. To disable the authentication, use the **no** form of this command.

authentication list *list-name*

no authentication list *list-name*

Syntax Description

list-name	Name of the list.

Defaults

An introducer is not authenticated.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

This command is used in SDP transactions. When the command is configured, the RADIUS or TACACS+ AAA server checks for a valid account by looking at the username and password.

The authentication list and the authorization list will usually both point to the same AAA list, but it is possible that the lists can be on different databases. This latter scenario is not recommended.

Examples

The following example shows that an authentication list named “authen-tac” has been configured. In this example, the authentication list is on a TACACS+ AAA server and the authorization list is on a RADIUS AAA server.

```
Router(config)# crypto wui tti registrar
Router(tti-registrar)# pki-server mycs
Router(tti-registrar)# authentication list authen-tac
Router(tti-registrar)# authorization list author-rad
Router(tti-registrar)# template username ftpuser password ftppwd
Router(tti-registrar)# template config ftp://ftp-server/iossnippet.txt
Router(tti-registrar)# end
```

Related Commands

Command	Description
authorization list (tti-registrar)	Specifies the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS CLI snippet that is sent back to the petitioner in an SDP operation.
debug crypto wui	Displays information about an SDP operation.

Command	Description
template config	Specifies a remote URL for a Cisco IOS CLI configuration template.
template username	Establishes a template username and password to access the configuration template on the file system.

authentication open

To enable open access on this port, use the **authentication open** command in interface configuration mode. To disable open access on this port, use the **no** form of this command.

authentication open

no authentication open

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	Support for this command was introduced.

Usage Guidelines

Open Access allows clients or devices to gain network access before authentication is performed.

You can verify your settings by entering the **show authentication** privileged EXEC command.

This command overrides the **authentication host-mode** *session-type* **open** global configuration mode command for the port only.

Examples

The following example shows how to enable open access to a port:

```
Router(config-if)# authentication open
Router(config-if)#
```

The following example shows how to enable open access to a port:

```
Router(config-if)# no authentication open
Router(config-if)#
```

Related Commands

Command	Description
show authentication	Displays Authentication Manager information.

authentication order

To specify the order in which the Auth Manager attempts to authenticate a client on a port, use the **authentication order** command in interface configuration mode. To return to the default authentication order, use the **no** form of this command.

authentication order {**dot1x** [**mab** | **webauth**] [**webauth**] | **mab** [**dot1x** | **webauth**] [**webauth**] | **webauth**}

no authentication order

Syntax Description

dot1x	Specifies IEEE 802.1X authentication.
mab	Specifies MAC-based authentication.
webauth	Specifies web-based authentication.

Command Default

The default authentication order is **dot1x**, **mab**, and **webauth**.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

Use the **authentication order** command to specify explicitly which authentication methods are run and the order in which they are run. Each method may be entered only once in the list and no method can be listed after **webauth**.

Examples

The following example sets the authentication order for a port:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet0/1
Switch(config-if)# authentication order mab dot1x
Switch(config-if)# end
Switch#
```

Related Commands

Command	Description
authentication priority	Specifies the priority of authentication methods.

authentication periodic

To enable automatic reauthentication on a port, use the **authentication periodic** command in interface configuration mode. To disable, use the **no** form of this command.

Note Effective with Cisco IOS Release 12.2(33)SXI, the **authentication periodic** command replaces the **dot1x reauthentication** command.

authentication periodic

no authentication periodic

Syntax Description

This command has no arguments or keywords.

Command Default

Reauthentication is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

Use the **authentication periodic** command to enable automatic reauthentication on a port. To configure the interval between reauthentication attempts, use the **authentication timer reauthenticate** command.

Examples

The following example enables reauthentication and sets the interval to 1800 seconds:

```
Switch(config)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet0/2
Switch(config-if)# authentication periodic
Switch(config-if)# authentication timer reauthenticate 1800
```

Related Commands

Command	Description
authentication timer reauthenticate	Specifies the period of time between attempts to reauthenticate an authorized port.

authentication port-control

To configure the authorization state of a controlled port, use the **authentication port-control** command in interface configuration mode. To disable the port-control value, use the **no** form of this command.

Note Effective with Cisco IOS Release 12.2(33)SXI, the **authentication port-control** command replaces the **dot1x port-control** command.

authentication port-control {**auto** | **force-authorized** | **force-unauthorized**}

no authentication port-control

Syntax Description

auto	Enables port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port.
force-authorized	Disables IEEE 802.1X on the interface and causes the port to change to the authorized state without requiring any authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The **force-authorized** keyword is the default.
force-unauthorized	Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.

Command Default

Ports authorized without authentication exchanges.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

To verify port-control settings, use the **show interfaces** command and check the Status column in the 802.1X Port Summary section of the display. An enabled status means that the port-control value is set to auto or to force-unauthorized.

The authentication process begins when the link state of the port transitions from down to up or when an EAPOL-start frame is received. The system requests the identity of the client and begins relaying authentication messages between the client and the authentication server.

Examples

The following specifies that the authorization status of the client will be determined by the authentication process:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Switch(config)# interface ethernet0/2
Switch(config-if)# authentication port-control auto
```

Related Commands

Command	Description
show interfaces	Displays information about interfaces.

authentication priority

To specify the priority of authentication methods on a port, use the **authentication priority** command in interface configuration mode. To return to the default, use the **no** form of this command.

authentication order {**dot1x** [**mab** | **webauth**] [**webauth**] | **mab** [**dot1x** | **webauth**] [**webauth**] | **webauth**}

no authentication order

Syntax Description

dot1x	Specifies IEEE 802.1X authentication.
mab	Specifies MAC-based authentication.
webauth	Specifies web-based authentication.

Command Default

The default priority order is **dot1x**, **mab**, and **webauth**.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

The **authentication order** command specifies the order in which authentication methods are attempted. This order is the default priority. To override the default priority and allow higher priority methods to interrupt a running authentication method, use the **authentication priority** command.

Examples

The following example configures the authentication order and the authentication priority on a port:

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# authentication order mab dot1x webauth
Switch(config-if)# authentication priority dot1x mab
Switch(config-if)# end
Switch#
```

Related Commands

Command	Description
authentication order	Specifies the order in which the Auth Manager attempts to authenticate a client on a port.

authentication terminal

To manually cut-and-paste certificate authentication requests, use the **authentication terminal** command in ca-profile-enroll configuration mode. To delete a current authentication request, use the **no** form of this command.

authentication terminal

no authentication terminal

Syntax Description

This command has no arguments or keywords.

Defaults

An authentication request is not specified.

Command Modes

Ca-profile-enroll configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

A user may manually cut-and-paste certificate authentication requests when a network connection between the router and certification authority (CA) is not available. After this command is enabled, the authentication request is printed on the console terminal so that it can be manually copied (cut) by the user.

Examples

The following example shows how to specify manual certificate authentication and certificate enrollment via HTTP:

```
crypto ca profile enrollment E
 authentication terminal
 enrollment terminal
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
crypto ca profile enrollment	Defines an enrollment profile.

authentication timer inactivity

To configure the time after which an inactive Auth Manager session is terminated, use the **authentication timer inactivity** command in interface configuration mode. To disable the inactivity timer, use the **no** form of this command.

authentication timer inactivity {*seconds* | **server**}

no authentication timer inactivity

Syntax Description

seconds	The period of inactivity, in seconds, allowed before an Auth Manager session is terminated and the port is unauthorized. The range is from 1 to 65535.
server	Specifies that the period of inactivity is defined by the Idle-Timeout value (RADIUS Attribute 28) on the authentication, authorization, and accounting (AAA) server.

Command Default

The inactivity timer is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

In order to prevent reauthentication of inactive sessions, use the **authentication timer inactivity** command to set the inactivity timer to an interval shorter than the reauthentication interval set with the **authentication timer reauthenticate** command.

Examples

The following example sets the inactivity interval on a port to 900 seconds:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface GigabitEthernet6/0
Switch(config-if)# authentication timer inactivity 900
Switch(config-if)# end
```

Related Commands

Command	Description
configuration timer reauthenticate	Specifies the time after which the Auth Manager attempts to reauthenticate an authorized port.
authentication timer restart	Specifies the interval after which the Auth Manager attempts to authenticate an unauthorized port.

authentication timer reauthenticate

To specify the period of time between which the Auth Manager attempts to reauthenticate authorized ports, use the **authentication timer reauthenticate** command in interface configuration mode. To reset the reauthentication interval to the default, use the **no** form of this command.

authentication timer reauthenticate {*seconds* | **server**}

no authentication timer reauthenticate

Syntax Description

seconds	The number of seconds between reauthentication attempts. The default is 3600.
server	Specifies that the interval between reauthentication attempts is defined by the Session-Timeout value (RADIUS Attribute 27) on the authentication, authorization, and accounting (AAA) server.

Command Default

The automatic reauthentication interval is set to 3600 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

Use the **authentication timer reauthenticate** command to set the automatic reauthentication interval of an authorized port. If you use the **authentication timer inactivity** command to configure an inactivity interval, configure the reauthentication interval to be longer than the inactivity interval.

Examples

The following example sets the reauthentication interval on a port to 1800 seconds:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface GigabitEthernet6/0
Switch(config-if)# authentication timer reauthenticate 1800
Switch(config-if)# end
```

Related Commands

Command	Description
authentication periodic	Enables automatic reauthentication.
authentication timer inactivity	Specifies the interval after which the Auth Manager ends an inactive session.
authentication timer restart	Specifies the interval after which the Auth Manager attempts to authenticate an unauthorized port.

authentication timer restart

To specify the period of time after which the Auth Manager attempts to authenticate an unauthorized port, use the **authentication timer restart** command in interface configuration mode. To reset the interval to the default value, use the **no** form of this command.

authentication timer restart *seconds*

no authentication timer restart

Syntax Description

seconds	The number of seconds between attempts to authenticate an unauthorized port. The range is 1 to 65535. The default is 60.

Command Default

No attempt is made to authenticate unauthorized ports.

Command Modes

Configuration interface (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

Use the **authentication timer restart** command to specify the interval between attempts to authenticate an unauthorized port. The default interval is 60 seconds.

Examples

The following example sets the authentication timer interval to 120 seconds:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface GigabitEthernet6/0
Switch(config-if)# authentication timer restart 120
Switch(config-if)# end
```

Related Commands

Command	Description
authentication timer inactivity	Specifies the period of time after which the Auth Manager attempts to authenticate an unauthorized port.
configuration timer reauthenticate	Specifies the time after which the Auth Manager attempts to reauthenticate an authorized port.

authentication trustpoint

To specify the trustpoint used to authenticate the Secure Device Provisioning (SDP) petitioner device's existing certificate, use the **authentication trustpoint** command in tti-registrar configuration mode. To change the specified trustpoint or use the default trustpoint, use the **no** form of this command.

authentication trustpoint {*trustpoint-label* | **use-any**}

no authentication trustpoint {*trustpoint-label* | **use-any**}

Syntax Description

trustpoint-label	Name of trustpoint.
use-any	Use any configured trustpoint.

Defaults

If this command is not specified, the petitioner-signing certificate is not verified.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Issue the **authentication trustpoint** command in tti-registrar configuration mode to validate the signing certificate that the petitioner used.

Examples

The following example shows how to specify the trustpoint mytrust for the petitioner-signing certificate:

```
crypto provisioning registrar
 authentication trustpoint mytrust
```

After the SDP exchange is complete, the petitioner automatically enrolls with the registrar and obtains a certificate. The following sample output from the **show running-config** command shows an automatically generated configuration with the default trustpoint tti:

```
crypto pki trustpoint tti
 enrollment url http://pki1-36a.cisco.com:80
 revocation-check crl
 rsakeypair tti 1024
 auto-enroll 70
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
crypto provisioning petitioner	Configures a device to become an SDP petitioner and enters tti-petitioner configuration mode.
trustpoint signing	Specifies the trustpoint associated with the SDP exchange between the petitioner and the registrar for signing the SDP data including the certificate.

authentication violation

To specify the action to be taken when a security violation occurs on a port, use the **authentication violation** command in interface configuration mode. To return to the default action, use the **no** form of this command.

authentication violation {**restrict** | **shutdown**}

no authentication violation

Syntax Description

restrict	Specifies that the port restrict traffic with the domain from which the security violation occurs.
shutdown	Specifies that the port shuts down upon a security violation.

Command Default

Ports are shut down when a security violation occurs.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

Use the **authentication violation** command to specify the action to be taken when a security violation occurs on a port.

Examples

The following example configures the GigabitEthernet interface to restrict traffic when a security violation occurs:

```
Switch(config)# interface GigabitEthernet6/2
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config-if)# authentication violation restrict
Switch(config-if)# end
```

authentication url

To specify the URL of the certification authority (CA) server to which to send authentication requests, use the **authentication url** command in ca-profile-enroll configuration mode. To delete the authentication URL from your enrollment profile, use the **no** form of this command.

authentication url *url*

no authentication url *url*

Syntax Description

url	URL of the CA server to which your router should send authentication requests. If you are using Simple Certificate Enrollment Protocol (SCEP) for enrollment, the *url* argument must be in the form http://CA_name, where CA_name is the host Domain Name System (DNS) name or IP address of the CA. If you are using TFTP for enrollment, the *url* argument must be in the form tftp://certserver/file_specification. (If the URL does not include a file specification, the fully qualified domain name [FQDN] of the router will be used.)

Defaults

Your router does not recognize the CA URL until you declare one using this command.

Command Modes

Ca-profile-enroll configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

If you do not specify the **authentication command** after you enable the **authentication url** command, the **authentication url** command functions the same as the **enrollment url** *url* command in trustpoint configuration mode. That is, the **authentication url** command will then be used only for certificate enrollment—not authentication.

This command allows the user to specify a different URL or a different method for authenticating a certificate and enrolling a certificate; for example, manual authentication and TFTP enrollment.

Examples

The following example shows how to configure an enrollment profile for direct HTTP enrollment with a CA server. In this example, the **authentication command** is also present.

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial
```

```
crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

The following example shows how to configure the enrollment profile named "E" to perform certificate authentication via HTTP and manual certificate enrollment:

```
crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment terminal
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
authentication command	Specifies the HTTP command that is sent to the CA for authentication.
crypto ca profile enrollment	Defines an enrollment profile.
enrollment	Specifies the enrollment parameters of your CA.

authorization

To enable authentication, authorization, and accounting (AAA) authorization for a specific line or group of lines, use the **authorization** command in line configuration mode. To disable authorization, use the **no** form of this command.

authorization {**arap** | **commands** *level* | **exec** | **reverse-access**} [**default** | *list-name*]

no authorization {**arap** | **commands** *level* | **exec** | **reverse-access**} [**default** | *list-name*]

Syntax Description

arap	Enables authorization for lines configured for AppleTalk Remote Access (ARA) protocol.
commands	Enables authorization on the selected lines for all commands at the specified privilege level.
level	Specific command level to be authorized. Valid entries are 0 through 15.
exec	Enables authorization to determine if the user is allowed to run an EXEC shell on the selected lines.
reverse-access	Enables authorization to determine if the user is allowed reverse access privileges.
default	(Optional) The name of the default method list, created with the **aaa authorization** command.
list-name	(Optional) Specifies the name of a list of authorization methods to use. If no list name is specified, the system uses the default. The list is created with the **aaa authorization** command.

Defaults

Authorization is not enabled.

Command Modes

Line configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

After you enable the **aaa authorization** command and define a named authorization method list (or use the default method list) for a particular type of authorization, you must apply the defined lists to the appropriate lines for authorization to take place. Use the **authorization** command to apply the specified method lists (or if none is specified, the default method list) to the selected line or group of lines.

Examples

The following example enables command authorization (for level 15) using the method list named charlie on line 10:

```
line 10
 authorization commands 15 charlie
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.

authorization (server-group)

To filter attributes in outbound Access Requests to the RADIUS server for purposes of authentication or authorization, use the **authorization** command in server-group configuration mode. To remove the filter on the authorization request or reply, use the **no** form of the command.

authorization [**request | reply**] [**accept | reject**] *list-name*

no authorization [**request | reply**] [**accept | reject**] *list-name*

Syntax Description

request	(Optional) Defines filters for outgoing authorization Access Requests.
reply	(Optional) Defines filters for incoming authorization Accept or Reject packets and for outgoing accounting requests.
accept	(Optional) Indicates that the required attributes and the attributes specified in the *list-name* argument will be accepted. All other attributes will be rejected.
reject	(Optional) Indicates that the attributes specified in the *list-name* will be rejected. All other attributes will be accepted.
list-name	Defines the given name for the accept or reject list.

Command Default

If specific attributes are not accepted or rejected, all attributes will be accepted.

Command Modes

Server-group configuration

Command History

Release	Modification
12.2(1)DX	This command was introduced.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(13)T	Platform support was added for the Cisco 7401ASR.
12.3(3)B	The **request** and **reply** keywords were added.
12.3(7)T	The **request** and **reply** keywords were integrated into Cisco IOS Release 12.3(7)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

An accept or reject list (also known as a filter) for RADIUS authorization allows users to configure the network access server (NAS) to restrict the use of specific attributes, thereby preventing the NAS from processing unwanted attributes.

Only one filter may be used for RADIUS authorization per server group.

Note The listname must be the same as the listname defined in the **radius-server attribute list** command, which is used with the **attribute (server-group configuration)** command to add to an accept or reject list.

Examples

The following example shows how to configure accept list "min-author" in an Access-Accept packet from the RADIUS server:

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
 server 10.1.1.1
 authorization accept min-author
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list min-author
 attribute 6-7
```

The following example shows that the attribute "all-attr" will be rejected in all outbound authorization Access Request messages:

```
aaa group server radius ras
 server 192.168.192.238 auth-port 1745 acct-port 1746
 authorization request reject all-attr
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict network access to the user.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
accounting (server-group configuration)	Specifies an accept or reject list for attributes that are to be sent to the RADIUS server in an accounting request.
attribute (server-group configuration)	Adds attributes to an accept or reject list.
radius-server attribute list	Defines an accept or reject list name.

authorization (tti-registrar)

To enable authentication, authorization, and accounting (AAA) authorization for an introducer or a certificate, use the **authorization** command in tti-registrar configuration mode. To disable authorization, use the **no** form of this command.

authorization {**login**} | {**certificate**} | {**login certificate**}

no authorization {**login**} | {**certificate**} | {**login certificate**}

Syntax Description

login	Use the username of the introducer for AAA authorization.
certificate	Use the certificate of the petitioner for AAA authorization.
login certificate	Use the username of the introducer and the certificate of the petitioner for AAA authorization.

Defaults

If an authorization list is configured, then authorization is enabled by default.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command controls the authorization of the introduction. Authorization can be based on the following:

- The login of the petitioner (username and password) to the registrar
- The current certificate of the petitioner
- Both the login of the introducer and the current certificate of the petitioner

If you issue the **authorization login** command, the introducer logs in with a username and password such as ttiuser and mypassword, which are used against the configured authorization list to contact the AAA server and determine the appropriate authorization.

If you issue the **authorization certificate** command, the certificate of the petitioner is used to build an AAA username, which is used to obtain authorization information.

If you issue the **authorization login certificate** command, authorization for the introducer combines with authorization for the petitioner's current certificate. This means that two AAA authorization lookups occur. In the first lookup, the introducer username is used to retrieve any AAA attributes associated with the introducer. The second lookup is done using the configured certificate name field. If an AAA attribute appears in both lookups, the second one prevails.

Examples

The following example shows how to specify authorization for both the introducer and the current certificate of the petitioner:

```
crypto provisioning registrar
 authorization login certificate
```

Related Commands

Command	Description
authorization list (tti-registrar)	Specifies the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS CLI snippet that is sent back to the petitioner for a user introducer in an SDP transaction.

authorization address ipv4

To specify a list of addresses for a Group Domain of Interpretation (GDOI) group, use the **authorization address ipv4** command in GDOI local server configuration mode. To remove an address from the group, use the **no** form of this command.

authorization address ipv4 {*access- list-name* | *access-list number*}

no authorization address ipv4 {*access- list-name* | *access-list number*}

Syntax Description

access-list-name	Name of an access control list (ACL).
access-list number	Standard IP access list number. Value: 1 through 99

Command Default

A list of addresses is not specified.

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

If the identity of the Internet Key Exchange (IKE) authentication matches an entry in the access control list, the address is authorized.

Examples

The following example shows that access list number 99 has been specified to be part of a GDOI group:

```
authorization address ipv4 99
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

authorization identity

To specify an authorization identity for a Group Domain of Interpretation (GDOI) group based on a distinguished name (DN) or Fully Qualified Domain Name (FQDN), use the **authorization identity** command in GDOI local server configuration mode. To delete a GDOI group authorization identity, use the **no** form of this command.

authorization identity *name*

no authorization identity *name*

Syntax Description

name	The name of the authorization identity, which can be a DN or FQDN.

Command Default

An authorization identity for a GDOI group is not defined.

Command Modes

GDOI local server configuration (gdoi-local-server)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Cisco Group Encrypted Transport Virtual Private Network (GET VPN) supports GDOI group member (GM) authorization using the **authorization identity** command when using Public Key Infrastructure (PKI) authentication between the GM and a key server (KS).

An authorization identity for a GDOI group is used to restrict registration of group members within a GDOI group. In order to successfully register with the KS, the DN or FQDN of the group members should match the configured identity string in this command. Use the **authorization identity** command to configure an authorization identity for a GDOI group.

Examples

The following example specifies an authorization identity using a DN called GETVPN_FILTER for the GETVPN GDOI group:

```
Router(config)# crypto gdoi group GETVPN
Router(config-gdoi-group)# server local
Router(gdoi-local-server)# authorization identity GETVPN_FILTER
Router(gdoi-local-server)# exit
Router(config-gdoi-group)# exit
Router(config)# crypto indentity GETVPN_FILTER
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
crypto identity	Configures the identity of a router with a given list of DNs in the certificate of the router.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

authoization list (global)

To specify the authentication, authorization, and accounting (AAA) authorization list, use the **authorization list** command in global configuration mode. To disable the authorization list, use the **no** form of this command.

authorization list *list-name*

no authorization list *list-name*

Syntax Description

list-name	Name of the AAA authorization list.

Defaults

An authorization list is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use the **authorization list** command to specify a AAA authorization list. For components that do not support specifying the application label, a default label of “any” from the AAA server will provide authorization. Likewise, a label of “none” from the AAA database indicates that the specified certificate is not valid. (The absence of any application label is equivalent to a label of “none,” but “none” is included for completeness and clarity.)

Examples

The following example shows that the AAA authorization list “maxaa” is specified:

```
aaa authorization network maxaaa group tacac+
aaa new-model
crypto ca trustpoint msca
enrollment url http://caserver.mycompany.com
 authorization list maxaa
 authorization username subjectname serialnumber
```

Related Commands

Command	Description
authorization username	Specifies the parameters for the different certificate fields that are used to build the AAA username.

authorization list (tti-registrar)

To specify the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS command-line interface (CLI) snippet that is sent back to the petitioner in an Secure Device Provisioning (SDP) operation, use the **authorization list** command in tti-registrar configuration mode. To disable the subject name and list of template variables, use the **no** form of this command.

authorization list *list-name*

no authorization list *list-name*

Syntax Description

list-name	Name of the list.

Defaults

There is no authorization list on the AAA server.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

This command is used in SDP operations. When the command is used, the RADIUS or TACACS+ AAA server stores the subject name and template variables. The name and variables are sent back to the petitioner in the Cisco IOS CLI snippets. This list and the authorization list are usually on the same database, but they can be on different AAA databases. (Storing lists on different databases is not recommended.)

When a petitioner makes an introducer request, multiple queries are sent to the AAA list database on the RADIUS or TACACS+ server. The queries search for entries of the following form:

```
user Password <userpassword>
   cisco-avpair="ttti:subjectname=<<DN subjectname>>"
   cisco-avpair="tti:iosconfig#<<value>>"
   cisco-avpair="tti:iosconfig#<<value>>"
   cisco-avpair="tti:iosconfig#=<<value>>"
```

Note The existence of a valid AAA username record is enough to pass the authentication check. The "cisco-avpair=tti" information is necessary only for the authorization check.

If a subject name was received in the authorization response, the TTI registrar stores it in the enrollment database, and that "subjectname" overrides the subject name that is supplied in the subsequent certificate request (PKCS10) from the petitioner device.

The numbered “tti:iosconfig” values are expanded into the TTI Cisco IOS snippet that is sent to the petitioner. The configurations replace any numbered ($1 through $9) template variable. Because the default Cisco IOS snippet template does not include the variables $1 through $9, these variables are ignored unless you configure an external Cisco IOS snippet template. To specify an external configuration, use the **template config** command.

Note The template configuration location may include a variable “$n,” which is expanded to the name with which the user is logged in.

Examples

The following example shows that the authorization list name is “author-rad.” In this example, the authentication list is on a TACACS+ AAA server and the authorization list is on a RADIUS AAA server.

```
Router(config)# crypto wui tti registrar
Router(tti-registrar)# pki-server mycs
Router(tti-registrar)# authentication list authen-tac
Router(tti-registrar)# authorization list author-rad
Router(tti-registrar)# template username ftpuser password ftppwd
Router(tti-registrar)# template config ftp://ftp-server/iossnippet.txt
Router(tti-registrar)# end
```

Related Commands

Command	Description
authentication list (tti-registrar)	Authenticates the introducer in an SDP operation.
debug crypto wui	Displays information about an SDP operation.
template config	Specifies a remote URL for a Cisco IOS CLI configuration template.
template username	Establishes a template username and password to access the configuration template on the file system.

authorization username

To specify the parameters for the different certificate fields that are used to build the authentication, authorization and accounting (AAA) username, use the **authorization username** command in global configuration mode. To disable the parameters, use the **no** form of this command.

authorization username {**subjectname** *subjectname*}

no authorization username {**subjectname** *subjectname*}

Syntax Description

subjectname	AAA username that is generated from the certificate subject name.
subjectname	Builds the username. The following are options that may be used as the AAA username: • **all**—Entire distinguished name (subject name) of the certificate. • **commonname**—Certificate common name. • **country**—Certificate country. • **email**—Certificate email. • **ipaddress**—Certificate ipaddress. • **locality**—Certificate locality. • **organization**—Certificate organization. • **organizationalunit**—Certificate organizational unit. • **postalcode**—Certificate postal code. • **serialnumber**—Certificate serial number. • **state**—Certificate state field. • **streetaddress**—Certificate street address. • **title**—Certificate title. • **unstructuredname**—Certificate unstructured name.

Defaults

Parameters for the certificate fields are not specified.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.3(11)T	The **all** option for the *subjectname* argument was added.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.

Examples

The following example shows that the serialnumber option is to be used as the authorization username:

```
aaa authorization network maxaaa group tacac+
aaa new-model
crypto ca trustpoint msca
enrollment url http://caserver.mycompany.com
 authorization list maxaaa
 authorization username subjectname serialnumber
```

Related Commands

Command	Description
authorization list	Specifies the AAA authorization list.

authorization username (tti-registrar)

To specify the parameters for the different certificate fields that are used to build the authentication, authorization, and accounting (AAA) username, use the **authorization username** command in tti-registrar configuration mode. To disable the parameters, use the **no** form of this command.

authorization username {**subjectname** *subjectname*}

no authorization username {**subjectname** *subjectname*}

Syntax Description

subjectname	AAA username that is generated from the certificate subject name.
subjectname	Builds the username. The following options can be used as the AAA username: • **all**—Entire distinguished name (subject name) of the certificate • **commonname**—Certificate common name • **country**—Certificate country • **email**—Certificate e-mail • **ipaddress**—Certificate IP address • **locality**—Certificate locality • **organization**—Certificate organization • **organizationalunit**—Certificate organizational unit • **postalcode**—Certificate postal code • **serialnumber**—Certificate serial number • **state**—Certificate state field • **streetaddress**—Certificate street address • **title**—Certificate title • **unstructuredname**—Certificate unstructured name

Defaults

Parameters for the certificate fields are not specified.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

The following example shows that the **serialnumber** option is used as the authorization username:

```
aaa authorization network maxaaa group tacac+
aaa new-model
```

```
crypto ca trustpoint msca
enrollment url http://caserver.mycompany.com
 authorization list maxaaa
 authorization username subjectname serialnumber
```

Related Commands

Command	Description
authorization list	Specifies the AAA authorization list.

authorize accept identity

To configure an identity policy profile, use the **authorize accept identity** command in parameter-map-type consent configuration mode. To remove an identity policy profile, use the **no** form of this command with the configured policy name.

authorize accept identity *identity-policy-name*

no authorize accept identity *identity-policy-name*

Syntax Description

identity-policy-name	Name of an identify profile.

Command Default

An identity policy does not exist.

Command Modes

Parameter-map-type consent (config-profile)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

If an identity policy is not configured, the interface policy will be used.

Examples

The following example shows how to configure accept policies within the consent-specific parameter maps:

```
parameter-map type consent consent_parameter_map
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity consent_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
parameter-map type consent default
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity test_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
```

auth-type

To set policy for devices that are dynamically authenticated or unauthenticated, use the **auth-type** command in identity profile configuration mode. To remove the policy that was specified, use the **no** form of this command.

auth-type {**authorize** | **not-authorize**} **policy** *policy-name*

no auth-type {**authorize** | **not-authorize**} **policy** *policy-name*

Syntax Description

authorize	Policy is specified for all authorized devices.
not-authorize	Policy is specified for all unauthorized devices.
policy *policy-name*	Specifies the name of the identity policy to apply for the associated authentication result.

Defaults

A policy is not set for authorized or unauthorized devices.

Command Modes

Identity profile configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

This command is used when a device is dynamically authenticated or unauthenticated by the network access device, and the device requires the name of the policy that should be applied for that authentication result.

Examples

The following example shows that 802.1x authentication applies to the identity policy “grant” for all dynamically authenticated hosts:

```
Router (config)# ip access-list extended allow-acl
Router (config-ext-nacl)# permit ip any any
Router (config-ext-nacl)# exit

Router (config)# identity policy grant
Router (config-identity-policy)# access-group allow-acl
Router (config-identity-policy)# exit

Router (config)# identity profile dot1x
Router (config-identity-prof)# auth-type authorize policy grant
```

Related Commands

Command	Description
identity policy	Creates an identity policy.
identity profile dot1x	Creates an 802.1x identity profile.

auth-type (ISG)

To specify the type of authorization Intelligent Services Gateway (ISG) will use for RADIUS clients, use the **auth-type** command in dynamic authorization local server configuration mode. To return to the default authorization type, use the **no** form of this command.

auth-type {**all** | **any** | **session-key**}

no auth-type {**all** | **any** | **session-key**}

Syntax Description

all	All attributes must match for authorization to be successful. This is the default.
any	Any attribute must match for authorization to be successful.
session-key	The session-key attribute must match for authorization to be successful. **Note** The only exception is if the session-id attribute is provided in the RADIUS Packet of Disconnect (POD) request, then the session ID is valid.

Command Default

All attributes must match for authorization to be successful.

Command Modes

Dynamic authorization local server configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

An ISG can be configured to allow external policy servers to dynamically send policies to the ISG. This functionality is facilitated by the Change of Authorization (CoA) RADIUS extension. CoA introduced peer to peer capability to RADIUS, enabling ISG and the external policy server each to act as a RADIUS client and server. Use the **auth-type** command to specify the type of authorization ISG will use for RADIUS clients.

Examples

The following example configures the ISG authorization type:

```
aaa server radius dynamic-author
 client 10.0.0.1
 auth-type any
```

Related Commands

Command	Description
aaa server radius dynamic-author	Configures an ISG as a AAA server to facilitate interaction with an external policy server.

auto-enroll

To enable certificate autoenrollment, use the **auto-enroll** command in ca-trustpoint configuration mode. To disable certificate autoenrollment, use the **no** form of this command.

auto-enroll [*percent*] [**regenerate**]

no auto-enroll [*percent*] [**regenerate**]

Syntax Description

percent	(Optional) The renewal percentage parameter, causing the router to request a new certificate after the specified percent lifetime of the current certificate is reached. If the percent lifetime is not specified, the request for a new certificate is made when the old certificate expires. The specified percent value must not be less than 10. If a client certificate is issued for less than the configured validity period due to the impending expiration of the certification authority (CA) certificate, the rollover certificate will be issued for the balance of that period. A minimum of 10 percent of the configured validity period, with an absolute minimum of 3 minutes is required, to allow rollover enough time to function.
regenerate	(Optional) Generates a new key for the certificate even if the named key already exists.

Command Default

Certificate autoenrollment is not enabled.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.3(7)T	The *percent* argument was added to support key rollover.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

Use the **auto-enroll** command to automatically request a router certificate from the CA that is using the parameters in the configuration. This command will generate a new Rivest, Shamir, and Adelman (RSA) key only if a new key does not exist with the requested label.

A trustpoint that is configured for certificate autoenrollment will attempt to reenroll when the router certificate expires.

Use the **regenerate** keyword to provide seamless key rollover for manual certificate enrollment. A new key pair is created with a temporary name, and the old certificate and key pair are retained until a new certificate is received from the CA. When the new certificate is received, the old certificate and key pair are discarded and the new key pair is renamed with the name of the original key pair. Some CAs require a new key for reenrollment to work.

If the key pair being rolled over is exportable, the new key pair will also be exportable. The following comment will appear in the trustpoint configuration to indicate whether the key pair is exportable:

```
! RSA keypair associated with trustpoint is exportable
```

Note If you are using a Secure Shell (SSH) service, you should set up specific RSA key pairs (different private keys) for the trustpoint and the SSH service. (If the Public Key Infrastructure [PKI] and the SSH infrastructure share the same default RSA key pair, a temporary disruption of SSH service could occur. The RSA key pair could become invalid or change because of the CA system, in which case you would not be able to log in using SSH. You could receive the following error message: "key changed, possible security problem.")

Examples

The following example shows how to configure the router to autoenroll with the CA named "trustme1" on startup. In this example, the **regenerate** keyword is issued, so a new key will be generated for the certificate. The renewal percentage is configured as 90; so if the certificate has a lifetime of one year, a new certificate is requested 36.5 days before the old certificate expires.

```
crypto ca trustpoint trustme1
 enrollment url http://trustme1.example.com/
 subject-name OU=Spiral Dept., O=example1.com
 ip-address ethernet0
 serial-number none
 auto-enroll 90 regenerate
 password revokeme
 rsakeypair trustme1 2048
 exit
crypto ca authenticate trustme1
```

Related Commands

Command	Description
crypto ca authenticate	Retrieves the CA certificate and authenticates it.
crypto ca trustpoint	Declares the CA that your router should use.

auto-rollover

To enable the automated certificate authority (CA) certificate rollover functionality, use the **auto-rollover** command in certificate server mode. To disable the automated rollover functionality, use the **no** form of this command.

auto-rollover [*time-period*]

no auto-rollover

Syntax Description

time-period	(Optional) Indicates when the shadow CA certificate should be generated in absolute time (not a percentage). Default is 30 calendar days before the expiration of the active private key infrastructure (PKI) root certificate.

Defaults

Automated CA rollover is not enabled.

Command Modes

Certificate server configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

CAs, like their clients, have certificates with expiration dates that have to be reissued when the current certificate is about to expire. CAs also have key pairs used to sign client certificates. When the CA certificate is expiring it must generate a new certificate and possibly a new key pair. This process, called rollover, allows for continuous operation of the network while clients and the certificate server are switching from an expiring CA certificate to a new CA certificate.

The command **auto-rollover** initiates the automatic CA certificate rollover process.

Examples

The following example shows how to configure automated CA certificate rollover.

```
Router(config)# crypto pki server mycs
Router(cs-server)# auto-rollover 25
Router(cs-server)# no shut

%Some server settings cannot be changed after CA certificate generation.
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
% Exporting Certificate Server signing certificate and keys...

% Certificate Server enabled.

Router(cs-server)#
```

With auto rollover enabled, the show crypto pki server command displays the current configuration of the certificate server.

```
Router# show crypto pki server
Certificate Server mycs:
    Status:enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name:CN=mycs
    CA cert fingerprint:70AFECA9 211CDDCC 6AA9D7FF 3ADB03AE
    Granting mode is:manual
    Last certificate issued serial number:0x1
    CA certificate expiration timer:00:49:26 PDT Jun 20 2008
    CRL NextUpdate timer:00:49:29 PDT Jun 28 2005
    Current storage dir:nvram:
    Database Level:Minimum - no cert data written to storage
    Auto-Rollover configured, overlap period 25 days
    Autorollover timer:00:49:26 PDT May 26 2008....
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate configuration mode.
show crypto pki server	Displays current state and configuration of the certificate server.

auto secure

To secure the management and forwarding planes of the router, use the **auto secure** command in privileged EXEC mode.

auto secure [**management** | **forwarding**] [**no-interact** | **full**] [**ntp** | **login** | **ssh** | **firewall** | **tcp-intercept**]

Syntax Description

management	(Optional) Only the management plane will be secured.
forwarding	(Optional) Only the forwarding plane will be secured.
no-interact	(Optional) The user will not be prompted for any interactive configurations. If this keyword is not enabled, the command will show the user the noninteractive configuration and the interactive configurations thereafter.
full	(Optional) The user will be prompted for all interactive questions. This is the default.
ntp	(Optional) Specifies the configuration of the Network Time Protocol (NTP) feature in the AutoSecure command line-interface (CLI).
login	(Optional) Specifies the configuration of the Login feature in the AutoSecure CLI.
ssh	(Optional) Specifies the configuration of the Secure Shell (SSH) feature in the AutoSecure CLI.
firewall	(Optional) Specifies the configuration of the firewall feature in the AutoSecure CLI.
tcp-intercept	(Optional) Specifies the configuration of the TCP-Intercept feature in the AutoSecure CLI.

Defaults

Autosecure is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)T.
12.3(4)T	The following keywords were added in Cisco IOS Release 12.3(4)T: **full**, **ntp**, **login**, **ssh**, **firewall**, and **tcp-intercept**.
12.3(8)T	Support for the roll-back functionality and system logging messages were added to Cisco IOS Release 12.3(8)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **auto secure** command allows a user to disable common IP services that can be exploited for network attacks by using a single CLI. This command eliminates the complexity of securing a router both by automating the configuration of security features and by disabling certain features that are enabled by default and that could be exploited for security holes.

Caution If you are using Security Device Manager (SDM), you must manually enable the HTTP server via the **ip http server** command.

This command takes you through a semi-interactive session (also known as the AutoSecure dialogue) in which to secure the management and forwarding planes. This command gives you the option to secure just the management or forwarding plane; if neither option is selected, the dialogue will ask you to configure both planes.

Caution If your device is managed by a network management (NM) application, securing the management plane could turn off vital services and disrupt the NM application support.

This command also allows you to go through all noninteractive configuration portions of the dialogue before the interactive portions. The noninteractive portions of the dialogue can be enabled by selecting the optional **no-interact** keyword.

Roll-back and System Logging Message Support

In Cisco IOS Release 12.3(8)T, support for roll-back of the AutoSecure configuration is introduced. Roll-back enables a router to revert back to its preautosecure configuration state if the AutoSecure configuration fails.

System Logging Messages capture any changes or tampering of the AutoSecure configuration that were applied on the running configuration.

Note Prior to Cisco IOS Release 12.3(8)T, roll-back of the AutoSecure configuration is unavailable; thus, you should always save the running configuration before configuring AutoSecure.

Examples

The following example shows how to enable AutoSecure to secure only the management plane:

```
Router# auto secure management
```

Related Commands

Command	Description
ip http server	Enables the HTTP server on your system, including the Cisco web browser user interface.
show auto secure config	Displays AutoSecure configurations.

auto-update client

To configure automatic update parameters for an Easy VPN remote device, use the **auto-update client** command in global configuration mode. To disable the parameters, use the **no** form of this command.

auto-update client {*type-of-system*} {**url** *url*} {**rev** *review-version*}

no auto-update client {*type-of-system*} {**url** *url*} {**rev** *review-version*}

Syntax Description

type-of-system	Free-format string (see Table 15).
url *url*	URL from which the Easy VPN device obtains the automatic update.
rev *review-version*	The version number is a comma-delimited string of acceptable versions.

Command Default

Automatic updates cannot occur.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

The URL is a generic way to specify the protocol, username, password, address of the server, directory, and filename. The format of a URL is as follows: protocol://username:password@server address:port/directory/filename.

The automatic update on the remote device is triggered only if the current version of the software is earlier than the one specified in the revision string. Otherwise, the automatic update is ignored.

Table 15 lists possible free-format strings to be used for the type-of-system argument.

Table 15 Possible Free-format Strings

Free-Format String	Operating System
Win	Microsoft Windows
Win95	Microsoft Windows 95
Win98	Microsoft Windows 98
WinNt	Microsoft Windows NT
Win2000	Microsoft Windows 2000
Linux	Linux

Table 15 Possible Free-format Strings

Free-Format String	Operating System
Mac	Macintosh
VPN3002	Cisco VPN 3002 Hardware Client

Examples

The following example shows update parameters have been set for a Windows 2000 operating system, a URL of http:www.ourcompanysite.com/newclient, and versions 3.0.1(Rel) and 3.1(Rel):

```
crypto isakmp client configuration group {group-name}
 auto-update client Win2000 url http:www.ourcompanysite.com/newclient rev 3.0.1(Rel),
  3.1(Rel)
```

backoff exponential

To configure the router for exponential backoff retransmit of accounting requests per RADIUS server group, enter the **backoff exponential** command in server-group RADIUS configuration mode. To disable this functionality, use the **no** form of this command.

backoff exponential [**max-delay** *minutes*] [**backoff-retry** *retransmits*]

no backoff exponential [**max-delay** *minutes*] [**backoff-retry** *retransmits*]

Syntax Description

max-delay *minutes*	(Optional) Number of retransmissions done in exponential max-delay mode. Valid range for the *minutes* argument is 1 through 120; if minutes is not specified, the default value (60 minutes) will be used.
backoff-retry *retransmits*	(Optional) Number of retransmissions done in exponential backoff mode in addition to normal and max-delay retransmissions. Valid range for the *retransmits* argument is 1 through 50; if retransmits is not specified, the default value (5 retransmits) will be used.

Command Default

This command is not enabled.

Command Modes

Server-group RADIUS configuration (config-sg-radius)

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Before enabling this command, you must configure the **aaa group server radius** command, which allows you to specify a server group and enter server-group RADIUS configuration mode.

The **backoff exponential** command allows you to configure an exponential backoff retransmission per RADIUS server group. That is, after the normally configured retransmission retries have been used, the router will keep on trying with an interval that doubles on each retransmit failure until a configured maximum interval is reached. This functionality allows you to retransmit accounting requests for many hours without overloading the RADIUS server when it does come back up.

Examples

The following example shows how to configure an exponential backoff retransmission:

```
aaa group server radius cat
 backoff exponential max-delay 90 backoff-retry 10
```

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
radius-server-backoff exponential	Configures the router for exponential backoff retransmit of accounting requests.

backup-gateway

To configure a server to "push down" a list of backup gateways to the client, use the **backup-gateway** command in global configuration mode. To remove a backup gateway, use the **no** form of this command.

backup-gateway {*ip-address* | *hostname*}

no backup-gateway {*ip-address* | *hostname*}

Syntax Description

ip-address	IP address of the gateway.
hostname	Host name of the gateway.

Defaults

A list of backup gateways is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

Before using the **backup-gateway** command, you must first configure the **crypto isakmp client configuration group** command.

An example of an attribute-value (AV) pair for the backup gateway attribute is as follows:

```
ipsec:ipsec-backup-gateway=10.1.1.1
```

Note

- If you have to configure more than one backup gateway, you have to add a **backup-gateway** command line for each.
- You can configure a maximum of 10 backup gateways.

Examples

The following example shows that gateway 10.1.1.1 has been configured as a backup gateway:

```
crypto isakmp client configuration group group1
 backup-gateway 10.1.1.1
```

The following output example shows that five backup gateways have been configured:

```
crypto isakmp client configuration group sdm
 key 6 RMZPPMRQMSdiZNJg`EBbCWTKSTi\d[
```

```
pool POOL1
acl 150
backup-gateway 172.16.12.12
backup-gateway 172.16.12.13
backup-gateway 172.16.12.14
backup-gateway 172.16.12.130
backup-gateway 172.16.12.131
max-users 250
max-logins 2
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.

banner

To configure an extended authentication (Xauth) banner string under a group policy definition, use the **banne**r command in global configuration mode. To disable the banner, use the **no** form of this command.

banner c {*banner-text*} **c**

no c {*banner-text*} **c**

Syntax Description

c	Delimiting character that must precede and follow the banner text. The delimiting character may be a character of your choice, such as "c" or "@."
banner-text	Text string of the banner. Maximum number of characters = 1024.

Command Default

If a banner is not configured, a banner will not be displayed.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

Examples

The following example shows that the banner "The quick brown fox jumped over the lazy dog" has been specified:

```
crypto isakmp client configuration group EZVPN
 banner @ The quick brown fox jumped over the lazy dog @
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.

banner (WebVPN)

To configure a banner to be displayed after a successful login, use the **banner** command in webvpn group policy configuration mode. To remove the banner from the policy group configuration, use the **no** form of this command.

banner *string*

no banner

Syntax Description

string	Text string that contains 7-bit ASCII values and HTML tags and escape sequences. The text banner must be in quotation marks if it contains spaces.

Command Default

A banner is not displayed after a successful login.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following example configures “Login Successful” to be displayed after login:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# banner “Login Successful”
Router(config-webvpn-group)#
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

base-dn

To configure a base distinguished name (DN) that you want to use to perform search operations in the Lightweight Directory Access Protocol (LDAP) server directory tree, use the **base-dn** command in LDAP server configuration mode. To delete a configured base DN for the LDAP server, use the **no** form of this command.

base-dn *string*

no base-dn *string*

Syntax Description

string	Distinguished name of the search base.

Command Default

No distinguished names are created.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command is valid only for LDAP servers. A base DN can take a form such as dc=example,dc=domain, where the base DN uses the Domain Name Server (DNS) domain name as its basis and is split into the domain components.

Examples

The following example shows how to configure the base DN for an LDAP server:

```
Router(config)# ldap server server1
Router(config-ldap-server)# base-dn "dc=sns,dc=example,dc=com"
```

Related Commands

Command	Description
ipv4 (**ldap**)	Creates an IPv4 address within an LDAP server address pool.
ldap server	Defines an LDAP server and enters LDAP server configuration mode.
transport port (**ldap**)	Configures the transport protocol for establishing a connection with the LDAP server.

bidirectional

To enable incoming and outgoing IP traffic to be exported across a monitored interface, use the **bidirectional** command in router IP traffic export (RITE) configuration mode. To return to the default functionality, use the **no** form of this command.

bidirectional

no bidirectional

Syntax Description

This command has no arguments or keywords.

Defaults

If this command is not enabled, only incoming traffic is exported.

Command Modes

RITE configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

By default, only incoming IP traffic is exported. If you choose to export outgoing IP traffic, you must issue both the **bidirectional** command, which enables outgoing traffic to be exported, and the **outgoing** command, which specifies how the outgoing traffic will be filtered.

The **ip traffic-export profile** command allows you to begin a profile that can be configured to export IP packets as they arrive or leave a selected router ingress interface. A designated egress interface exports the captured IP packets out of the router. Thus, the router can export unaltered IP packets to a directly connected device.

Examples

The following example shows how to export both incoming and outgoing IP traffic on the FastEthernet interface:

```
Router(config)# ip traffic-export profile johndoe
Router(config-rite)# interface FastEthernet1/0.1
Router(config-rite)# bidirectional
Router(config-rite)# incoming access-list 101
Router(config-rite)# outgoing access-list 101
Router(config-rite)# mac-address 6666.6666.3333
```

Related Commands

Command	Description
interface (RITE)	Specifies the outgoing interface for exporting traffic.
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.
outgoing	Configures filtering for outgoing export traffic.

binary file

To specify the binary file location on the registrar and the destination binary file location on the petitioner, use the **binary file** command in tti-registrar configuration mode.

binary file *sourceURL destinationURL*

Syntax Description

sourceURL	Specifies the source URL on the registrar for the binary file using one of the keywords in Table 15.
destinationURL	Specifies the destination URL on the petitioner for binary file using one of the keywords in Table 15.

Command Default

None

Command Modes

tti-registrar configuration (tti-registrar)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Use the **binary file** command to specify the location where a binary file will be retrieved from and copied to during the Trusted Transitive Introduction (TTI) exchange. There may be up to nine binary files transferred, each with a different source and destination location. A destination URL could also be a token on the petitioner, such as usbtoken0:

The binary files are retrieved from the registrar and copied to the petitioner. Source URLs for the binary file location are expanded on the registrar. Destination URLs are expanded on the petitioner. Binary files are not processed through the binary expansion functions.

Table 16 Source and Destination URL Keywords

Keyword	Description
archive:	Retrieves from the archive location.
cns:	Retrieves from the Cisco Networking Services (CNS) configuration engine.
disk0:	Retrieves from disk0.
disk1:	Retrieves from disk1.
flash:	Retrieves from flash memory.
ftp:	Retrieves from the FTP network server.
http:	Retrieves from a HTTP server.
https:	Retrieves from a Secure HTTP (HTTPS) server.
null:	Retrieves from the file system.
nvram:	Retrieves from the NVRAM of the router.

Table 16 Source and Destination URL Keywords

Keyword	Description
rcp:	Retrieves from a remote copy (rcp) protocol network server.
scp:	Retrieves from a network server that supports Secure Shell (SSH).
system:	Retrieves from system memory, which includes the running configuration.
tar:	Retrieves from a compressed file in tar format.
tftp:	Retrieves from a TFTP network server.
tmpsys:	Retrieves from a temporary system location.
unix:	Retrieves from the UNIX system location.
usbtoken:	Retrieves from the USB token.

Examples

The following example shows how to specify on the registrar where the source binary files are located and where the binary files will be copied to on the petitioner:

```
crypto provisioning registrar
  pki-server cs1
  binary file http://myserver/file1 usbtoken0://file1
  binary file http://myserver/file2 flash://file2
```

Related Commands

Command	Description
crypto provisioning registrar	Configures a device to become a secure device provisioning (SDP) registrar and enter tti-registrar configuration mode.
template file	Specifies the source template file location on the registrar and the destination template file location on the petitioner.

bind authenticate

To authenticate the client to a Lightweight Directory Access Protocol (LDAP) server, use the **bind authenticate** command in LDAP server configuration mode. To disable authenticated bind and to allow anonymous bind, use the **no** form of this command.

bind authenticate root-dn *username* **password** [**0** *string* | **7** *string*] *string*

no bind authenticate root-dn *username* **password** [**0** *string* | **7** *string*] *string*

Syntax Description

root-dn	Specifies the bind distinguished name (DN) for an authenticated user.
username	Root user of the LDAP server.
password	Specifies the LDAP server password.
0	(Optional) Specifies the unencrypted (cleartext) shared key.
7	(Optional) Specifies the hidden shared key.
string	The unencrypted (cleartext) shared key.

Command Default

Anonymous bind is performed. Anonymous bind refers to a simple bind operation with no DN and password.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Examples

The following example shows how to authenticate the user named user1 to the LDAP server using the password 123:

```
Router(config)# ldap server server1
Router(config-ldap-server)# bind authenticate root-dn
cn=user1,cn=users,dc=nac-blr2,dc=example,dc=com password 123
```

Related Commands

Command	Description
ipv4 (**ldap**)	Creates an IPv4 address within an LDAP server address pool.
ldap server	Defines an LDAP server and enters LDAP server configuration mode.
transport port (**ldap**)	Configures the transport protocol for establishing a connection with the LDAP server.

block count

To lock out group members for a length of time after a set number of incorrect passwords are entered, use the **block count** command in local RADIUS server group configuration mode. To remove the user block after invalid login attempts, use the **no** form of this command.

block count *count* **time** {*seconds* | **infinite**}

no block count *count* **time** {*seconds* | **infinite**}

Syntax Description

count	Number of failed passwords that triggers a lockout. Range is from 1 to 4294967295.
time	Specifies the time to block the account.
seconds	Number of seconds that the lockout should last. Range is from 1 to 4294967295.
infinite	Specifies the lockout is indefinite.

Defaults

No default behavior or values

Command Modes

Local RADIUS server group configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

If the **infinite** keyword is entered, an administrator must manually unblock the locked username.

Examples

The following command locks out group members for 120 seconds after three incorrect passwords are entered:

```
Router(config-radsrv-group)# block count 3 time 120
```

Related Commands

Command	Description
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.

Command	Description
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

browser-attribute import

To import user-defined browser attributes into a webvpn context, use the **browser-attribute import** command in webvpn context configuration mode. To remove a browser attribute, use the **no** form of this command.

browser-attribute import *device*:*file*

no browser-attribute import *device*:*file*

Syntax Description

device:*file*	• *device*:—Storage device on the system. • *file*—Name of file to be imported. The file name should include the directory location.

Command Default

Default values of the attributes are used.

Command Modes

Webvpn context configuration (config-webvpn-context)

Command History

Release	Modification
12.4(22)T	This command was introduced. Attributes that are currently supported are primary color, secondary color, text color, secondary text color, login-message, browser title, and title color.

Usage Guidelines

This command will override any other browser attributes that have already been configured using command-line interface (CLI).

Examples

The following example shows that the file “test-attr.xml” is to be imported from flash:

```
Router (config)# webvpn context sslvpn
 Router (config-webvpn-context)# browser-attribute import flash:test-attr.xml
```

Related Commands

Command	Description
webvpn create template	Creates templates for multilanguage support for messages in an SSL VPN.

browser-proxy

To apply browser-proxy parameter settings to a group, use the **browser-proxy** command in ISAKMP group configuration mode. To disable the parameter settings, use the **no** form of this command.

browser-proxy {*browser-proxy-map-name*}

no browser-proxy {*browser-proxy-map-name*}

Syntax Description

browser-proxy-map-name	Name of the browser proxy.

Command Default

Browser-proxy settings are not applied to a group.

Command Modes

ISAKMP group configuration (config-isakmp-group)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

Ensure that you define the browser proxy name before you define the crypto Internet Security Association and Key Management Protocol (ISAKMP) client configuration group name. The two names have to be the same.

Examples

The following example shows that browser proxy map “EZVPN” has been applied to the group “EZVPN”:

```
crypto isakmp client configuration group EZVPN
 browser-proxy EZVPN
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.

ca trust-point

To identify the trustpoints that is used to validate a certificate during Internet Key Exchange (IKE) authentication, use the **ca trust-point** command in ISAKMP profile configuration mode. To remove the trustpoint, use the **no** form of this command.

ca trust-point *trustpoint-name*

no ca trust-point *trustpoint-name*

Syntax Description

trustpoint-name	The trustpoint name as defined in the global configuration.

Defaults

If there is no trustpoint defined in the Internet Security Association and Key Management Protocol (ISAKMP) profile configuration, the default is to validate the certificate using all the trustpoints that are defined in the global configuration.

Command Modes

ISAKMP profile configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **ca trust-point** command can be used multiple times to define more than one trustpoint.

This command is useful when you want to restrict validation of certificates to a list of trustpoints. For example, the router global configuration has two trustpoints, A and B, which are trusted by VPN1 and VPN2, respectively. Each Virtual Private Network (VPN) wants to restrict validation only to its trustpoint.

Before you can use this command, you must enter the **crypto isakmp profile** command.

Note A router initiating IKE and a router responding to the IKE request should have symmetrical trustpoint configurations. For example, a responding router (in IKE Main Mode) performing RSA signature encryption and authentication might use trustpoints that were defined in the global configuration when sending the CERT-REQ payloads. However, the router might use a restricted list of trustpoints that were defined in the ISAKMP profile for the certificate verification. If the peer (the IKE initiator) is configured to use a certificate whose trustpoint is in the global list of the responding router but not in ISAKMP profile of the responding router, the certificate is rejected. (However, if the initiating router does not know about the trustpoints in the global configuration of the responding router, the certificate can still be authenticated.)

Examples

The following example specifies two trustpoints, A and B. The ISAKMP profile configuration restricts each VPN to one trustpoint.

```
crypto ca trustpoint A
enrollment url http://kahului:80
crypto ca trustpoint B
enrollment url http://arjun:80
!
crypto isakmp profile vpn1
 trustpoint A
!
crypto isakmp profile vpn2
 ca trust-point B
```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile.

cache authentication profile (server group configuration)

To specify a cache authentication profile to use in a named RADIUS or TACACS+ server group, use the **cache authentication profile** command in server group configuration mode. To disable an authentication cache profile, use the **no** form of this command.

cache authentication profile *name*

no cache authentication profile *name*

Syntax Description

name	Name of an authentication cache profile.

Command Default

No authentication cache profile is enabled.

Command Modes

Server group configuration (config-sg-radius)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use this command to specify a cache authentication profile for a RADIUS or TACACS+ server group.

Configure the authentication profile prior to applying it to a RADIUS or TACACS+ server group to avoid an error message.

Examples

The following example caches authentication responses from a RADIUS server according to the rules configured in the authentication profile authen-profile:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa group server radius networkauthentications
Router(config-sg-radius)# cache authentication profile authen-profile
```

Related Commands

Command	Description
cache authorization profile	Specifies an authorization cache profile to use in a named RADIUS or TACACS+ server group.

cache authorization profile (server group configuration)

To specify a cache authorization profile to use in a named RADIUS or TACACS+ server group, use the **cache authorization profile** command in server group configuration mode. To disable an authorization cache profile, use the **no** form of this command.

cache authorization profile *name*

no cache authorization profile *name*

Syntax Description

name	Name of a cache authorization profile to apply to either a RADIUS or TACACS+ server group.

Command Default

No authorization cache profile is enabled.

Command Modes

Server group configuration (config-sg-radius)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use this command to specify an authorization profile for a RADIUS or TACACS+ server group.

Examples

The following example caches authorization responses from a RADIUS server according to the rules configured in the authorization profile author-profile:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa group server radius authorizations
Router(config-sg-radius)# cache authorization profile author-profile
```

The authorization profile author-profile must be configured prior to applying it to a RADIUS or TACACS+ server group or an error message is generated.

Related Commands

Command	Description
cache authentication profile	Specifies an authentication cache profile to use in a named RADIUS or TACACS+ server group.

cache clear age

To specify when, in minutes, cache entries expire and the cache is cleared, use the **cache clear age** command in AAA filter configuration mode. To return to the default value, use the **no** form of this command.

cache clear age *minutes*

no cache clear age

Syntax Description

minutes	Any value from 0 to 4294967295; the default value is 1440 minutes.

Defaults

1440 minutes (1 day)

Command Modes

AAA filter configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

After enabling the **aaa cache filter** command, which allows you to configure cache filter parameters, you can use the **cache clear age** command to specify when cache entries should expire. If this command is not specified, the default value (1440 minutes) will be enabled.

Examples

The following example shows how to configure the cache entries to expire every 60 minutes:

```
aaa cache filter
 cache clear age 60
```

Related Commands

Command	Description
aaa cache filter	Enables filter cache configuration.

cache disable

To disable the cache, use the **cache disable** command in AAA filter configuration mode. To return to the default, use the **no** form of this command.

cache disable

no cache disable

Syntax Description

This command has no arguments or keywords.

Defaults

Caching is enabled.

Command Modes

AAA filter configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

After enabling the **aaa cache filter** command, which allows you to configure cache filter parameters, you can use the **cache disable** command to disable filter caching. This command can be used to verify that the access control lists (ACLs) are being downloaded.

Examples

The following example shows how to disable filter caching:

```
aaa cache filter
 cache disable
```

Related Commands

Command	Description
aaa cache filter	Enables filter cache configuration.

cache expiry (server group configuration)

To configure how long cached database profile entries in RADIUS or TACACS+ server groups are stored before they expire, use the **cache expiry** command in server group configuration mode. To reset the expiration time to the default value, use the **no** form of this command.

cache expiry *hours* [**enforce** | **failover**]

no cache expiry

Syntax Description

hours	Length of time, in hours, for a cache database profile entry to expire. Range is from 0 to 2147483647. Default is 24 hours.
enforce	(Optional) Specifies to not use expired entries.
failover	(Optional) Specifies to use an expired entry if all other methods fail.

Command Default

Cache entries expire in 24 hours.

Command Modes

Server group configuration (config-sg-radius)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use this command to set the amount of time before a cache entry expires (becomes stale). A stale entry is still usable, but the entry will, by default, revise its record with more updated information.

Examples

The following example sets the expiry time for cache profile entries to 10 days such that the expired entries cannot be used:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa group server radius networkusers
Router(config-sg-radius)# cache expiry 240 enforce
```

Related Commands

Command	Description
cache authentication profile	Specifies an authentication cache profile to use in a named RADIUS or TACACS+ server group.
cache authorization profile	Specifies an authorization cache profile to use in a named RADIUS or TACACS+ server group.

cache max

To limit the absolute number of entries that a cache can maintain for a particular server, use the **cache max** command in AAA filter configuration mode. To return to the default value, use the **no** form of this command.

cache max *number*

no cache max

Syntax Description

number	Maximum number of entries the cache can maintain. Any value from 0 to 4294967295; the default value is 100 entries.

Defaults

100 entries

Command Modes

AAA filter configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

After enabling the **aaa cache filter** command, which allows you to configure cache filter parameters, you can use the **cache max** command to specify the maximum number of entries the cache can have at any given time. If this command is not specified, the default value (100 entries) will be enabled.

Examples

The following example shows how to configure the cache to maintain a maximum of 150 entries:

```
aaa cache filter
 password mycisco
 cache max 150
```

Related Commands

Command	Description
aaa cache filter	Enables filter cache configuration.

cache refresh

To refresh a cache entry after a new session begins, use the **cache refresh** command in AAA filter configuration mode. To disable this functionality, use the **no** form of this command.

cache refresh

no cache refresh

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

Command Modes

AAA filter configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The **cache refresh** command is used in an attempt to keep cache entries from the filter server, that are being referred to by new sessions, within the cache. This command resets the idle timer for these entries when they are referenced by new calls.

Examples

The following example shows how to disable the **cache refresh** command:

```
aaa cache filter
 password mycisco
 no cache refresh
 cache max 100
```

Related Commands

Command	Description
aaa cache filter	Enables filter cache configuration.

call admission limit

To instruct Internet Key Exchange (IKE) to drop security association (SA) requests (that is, calls for Call Admission Control [CAC]) when a specified level of system resources is being consumed, use the **call admission limit** command in global configuration mode. To disable this feature, use the **no** form of this command.

call admission limit *charge*

no call admission limit *charge*

Syntax Description

charge	Level of the system resources that, when used, causes IKE to stop accepting new SA requests. Valid values are 1 to 100000.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

To prevent IKE processes from using excessive CPU resources, you can set a limit value depending on the network topology, the capabilities of the router, and the traffic patterns.

Examples

The following example causes IKE to drop calls when a given level of system resources are being used:

```
Router(config)# call admission limit 90000
```

Related Commands

Command	Description
call admission load	Configures a CAC metric for scaling WAN protocol session load.
crypto call admission limit	Specifies the maximum number of IKE SAs that the router can establish before IKE begins rejecting new SA requests.
show call admission statistics	Monitors the global CAC configuration parameters and the behavior of CAC.

call guard-timer

To set a guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request, use the **call guard-timer** command in controller configuration mode. To remove the **call guard-timer** command from your configuration file, use the **no** form of this command.

call guard-timer *milliseconds* [**on-expiry** {**accept** | **reject**}]

no call guard-timer *milliseconds* [**on-expiry** {**accept** | **reject**}]

Syntax Description

milliseconds	Specifies the number of milliseconds to wait for a response from the RADIUS server.
on-expiry accept	(Optional) Accepts the call if a response is not received from the RADIUS server within the specified time.
on-expiry reject	(Optional) Rejects the call if a response is not received from the RADIUS server within the specified time.

Defaults

No default behavior or values.

Command Modes

Controller configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows a guard timer that is set at 20000 milliseconds. A call will be accepted if the RADIUS server has not responded to a preauthentication request when the timer expires.

```
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 ds0-group 0 timeslots 1-24 type e&m-fgb dtmf dnis
 cas-custom 0
  call guard-timer 20000 on-expiry accept

aaa preauth
group radius
  dnis required
```

Related Commands

Command	Description
aaa preauth	Enters AAA preauthentication configuration mode.

category (ips)

To specify a signature category that is to be used for multiple signature actions or conditions, use the **category** command in IPS-category configuration mode.

category *category* [*sub-category*]

Syntax Description

category	Category name. For a list of supported top-level categories, use the router CLI help (**?**).
sub-category	(Optional) Category submode. Submode categories are dependent on the category type; that is, submode categories vary from category to category. For a list of supported submode categories, use the router CLI help (**?**).

Command Default

None

Command Modes

IPS-category configuration (config-ips-category)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Cisco IOS Intrusion Prevention System (IPS) 5.x uses signatures and signature categories. All signatures are pregrouped into categories; the categories are hierarchical. An individual signature can belong to more than one category. Top-level categories help to define general types of signatures. Subcategories exist beneath each top-level signature category.

Examples

The following example shows how to tune event-action parameters for the signature category "adware/spyware." All tuning information will be applied to all signatures that belong to the adware/spyware category.

```
Router(config)# ip ips signature-category
Router(config-ips-category)# category attack adware/spyware
Router(config-ips-category-action)# event-action produce-alert
Router(config-ips-category-action)# event-action deny-packet-inline
Router(config-ips-category-action)# event-action reset-tcp-connection
Router(config-ips-category-action)# retired false
Router(config-ips-category-action)# ^Z
Do you want to accept these changes? [confirm]y
```

Related Commands

Command	Description
ip ips signature-category	Enters IPS category (config-ips-category) configuration mode, which allows you to tune Cisco IOS IPS signature parameters on the basis of a signature category.

cdp-url

To specify a certificate revocation list (CRL) distribution point (CDP) to be used in certificates that are issued by the certificate server, use the **cdp-url** command in certificate server configuration mode. To remove a CDP from your configuration, use the **no** form of this command.

cdp-url *url*

no cdp-url *url*

Syntax Description

url	HTTP URL where CRLs are published.

Command Default

When verifying a certificate that does not have a specified CDP, Cisco IOS public key infrastructure (PKI) clients will use Simple Certificate Enrollment Protocol (SCEP) to retrieve the CRL directly from their configured certificate server.

Command Modes

Certificate server configuration (cs-server)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

CRLs can be distributed via SCEP, which is the default method, or a CDP, if configured and available. If you set up a CDP, use the **cdp-url** command to specify the CDP location. The CDP URL may be changed after the certificate server is running, but existing certificates will not be reissued with the new CDP that is specified via the **cdp-url** command.

You may specify the CDP location by a simple HTTP URL string for example,

cdp-url http://server.company.com/ca1.crl

The certificate server supports only one CDP; thus, all certificates that are issued include the same CDP.

If you have PKI clients that are not running Cisco IOS software and that do not support a SCEP GetCRL request, you can specify a non-SCEP request for the retrieval of the CRL from the certificate server by specifying **cdp-url** command with the URL in the following format where *cs-addr* is the location of the certificate server:

cdp-url http://*cs-addr*/cgi-bin/pkiclient.exe?operation=GetCRL

Note If your Cisco IOS certificate authority (CA) is also configured as your HTTP CDP server, specify your CDP with the **cdp-url** http://*cs-addr*/cgi-bin/pkiclient.exe?operation=GetCRL command syntax.

It is the responsibility of the network administrator to ensure that the CRL is available from the location that is specified via the **cdp-url** command.

In order to force the parser to retain the embedded question mark within the specified location, enter Ctrl-v prior to the question mark. If this action is not taken, CRL retrieval via HTTP will return an error message.

Examples

The following example shows how to configure a CDP location where the PKI clients do not support SCEP GetCRL requests:

```
Router(config)# crypto pki server aaa
Router(cs-server)# database level minimum
Router(cs-server)# database url tftp://10.1.1.1/username1/
Router(cs-server)# issuer-name CN=aaa
Router(cs-server)# cdp-url http://server.company.com/certEnroll/aaa.crl
```

The following example shows how to configure a CDP location where the PKI clients support SCEP GetCRL requests:

```
Router(config)# crypto pki server aaa
Router(cs-server)# database level minimum
Router(cs-server)# database url tftp://10.1.1.1/username1 /
Router(cs-server)# issuer-name CN=aaa
Router(cs-server)# cdp-url http://aaa/cgi-bin/pkiclient.exe?operation=GetCRL
```

Verifying a CDP Configuration

The following example is sample output from the **show crypto ca certificates** command, which allows you to verify the specified CDP. In this example, the CDP is "http://msca-root.cisco.com/certEnroll/aaa.crl."

```
Router# show crypto ca certificates

Certificate
  Status: Available
  Certificate Serial Number: 03
  Certificate Usage: General Purpose
  Issuer:
    CN = aaa
  Subject:
    Name: Router.cisco.com
    OID.1.2.840.113549.1.9.2 = Router.cisco.com
  CRL Distribution Point:
    http://msca-root.cisco.com/certEnroll/aaa.crl
  Validity Date:
    start date: 18:44:49 GMT Jun 6 2003
    end   date: 18:44:49 GMT Jun 5 2004
    renew date: 00:00:00 GMT Jan 1 1970
  Associated Trustpoints: bbb
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.
crypto pki server revoke	Revokes a certificate based on its serial number.
lifetime crl	Defines the lifetime of the CRL that is used by the certificate server.
show crypto ca certificates	Displays information about your certificate, the certification authority certificate, and any registration authority certificates.

certificate

To manually add certificates, use the **certificate** command in certificate chain configuration mode. To delete your router's certificate or any registration authority certificates stored on your router, use the **no** form of this command.

certificate *certificate-serial-number*

no certificate *certificate-serial-number*

Syntax Description

certificate-serial-number	Serial number of the certificate to add or delete.

Defaults

No default behavior or values.

Command Modes

Certificate chain configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You could use this command to manually specify a certificate. However, this command is rarely used in this manner. Instead, this command is usually used only to add or delete certificates.

Examples

The following example deletes the router's certificate. In this example, the router had a general purpose RSA key pair with one corresponding certificate. The **show** command is used in this example to determine the serial number of the certificate to be deleted.

```
myrouter# show crypto ca certificates

Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: 0123456789ABCDEF0123456789ABCDEF
  Key Usage: General Purpose

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set

myrouter# configure terminal
```

```
myrouter(config)# crypto ca certificate chain myca
myrouter(config-cert-chain)# no certificate 0123456789ABCDEF0123456789ABCDEF
% Are you sure you want to remove the certificate [yes/no]? yes
% Be sure to ask the CA administrator to revoke this certificate.
myrouter(config-cert-chain)# exit
```

Related Commands

Command	Description
crypto ca certificate chain	Enters the certificate chain configuration mode.

chain-validation

To configure the level to which a certificate chain is processed on all certificates, including subordinate certificate authority (CA) certificates, use the **chain-validation** command in ca-trustpoint configuration mode. To revert to the command default, use the **no** form of this command.

chain-validation [{**stop** | **continue**} [*parent-trustpoint*]]

no chain-validation [{**stop** | **continue**} [*parent-trustpoint*]]

Syntax Description

stop	(Optional) Specifies that the certificate is already trusted. This is the default setting.
continue	(Optional) Specifies that the subordinate CA certificate associated with the trustpoint must be validated.
parent-trustpoint	(Optional) The name of the CA parent trustpoint.

Command Default

Certificate chain path processing continues until the first trusted certificate, or trustpoint, is reached.

Command Modes

Ca-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

Configuring the level to which a certificate chain is processed allows for the reauthentication of trusted certificates, the extension of a trusted certificate chain, or the completion of a certificate chain that contains a gap. Devices must be enrolled in your PKI hierarchy and the appropriate key pair associated with the certificate.

If there is more than one parent trustpoint configured, Cisco IOS will select a parent trustpoint based upon configured settings to validate the certificate chain. If you want a specific parent trustpoint to validate certificates, then that trustpoint must be configured with the *parent-trustpoint* argument specified. All certificates, peer and subordinate CA certificates, are validated in the same manner. All trustpoint settings—ACLs, AAA authorization lists, CDP or OCSP overrides—will apply, as will trustpoint policies for trusted and untrusted certificates.

A trustpoint associated with the root CA cannot be configured to be validated to the next level. If **chain-validation continue** is configured for the trustpoint associated with the root CA, an error message will be displayed and the chain validation will revert to the default **chain-validation stop**.

Examples

In the following configuration example, all of the certificates will be validated—the peer, SubCA11, SubCA1, and RootCA certificates.

```
crypto pki trustpoint RootCA
 enrollment terminal
 chain-validation stop
 revocation-check none
 rsakeypair RootCA

crypto pki trustpoint SubCA1
 enrollment terminal
 chain-validation continue RootCA
 revocation-check none
 rsakeypair SubCA1

crypto pki trustpoint SubCA11
 enrollment terminal
 chain-validation continue SubCA1
 revocation-check none
 rsakeypair SubCA11
```

In the following configuration example, the following certificates will be validated—the peer and SubCA1 certificates.

```
crypto pki trustpoint RootCA
 enrollment terminal
 chain-validation stop
 revocation-check none
 rsakeypair RootCA

crypto pki trustpoint SubCA1
 enrollment terminal
 chain-validation continue RootCA
 revocation-check none
 rsakeypair SubCA1


crypto pki trustpoint SubCA11
 enrollment terminal
 chain-validation continue SubCA1
 revocation-check none
 rsakeypair SubCA11
```

In the following configuration example, SubCA1 is not in the configured Cisco IOS hierarchy but is expected to have been supplied in the certificate chain presented by the peer.

If the peer sends SubCA1, SubCA11, and the peer certificates in the certificate chain, the following certificates will be validated—the peer, SubCA11, and SubCA1 certificates.

If the peer does not supply the SubCA1 certificate in the presented certificate chain, the chain validation will fail.

```
crypto pki trustpoint RootCA
 enrollment terminal
 chain-validation stop
 revocation-check none
 rsakeypair RootCA

crypto pki trustpoint SubCA11
 enrollment terminal
 chain-validation continue RootCA
 revocation-check none
 rsakeypair SubCA11
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the CA that your router should use.
revocation-check	Checks the revocation status of a certificate.

cifs-url-list

To enter webvpn URL list configuration mode to configure a list of Common Internet File System (CIFS) server URLs to which a user has access on the portal page of a Secure Sockets Layer Virtual Private Network (SSL VPN) and to attach the URL list to a policy group, use the **cifs-url-list** command in webvpn context configuration and webvpn group policy configuration mode, respectively. To remove the CIFS server URL list from the SSL VPN context configuration and from the policy group, use the **no** form of this command.

cifs-url-list *name*

no cifs-url-list *name*

Syntax Description

name	Name of the URL list. The list name can up to 64 characters in length.

Command Default

Webvpn URL list configuration mode is not entered, and a list of URLs to which a user has access on the portal page of an SSL VPN website is not configured. If the command is not used to attach a CIFS server URL list to a policy group, then a URL list is not attached to a group policy.

Command Modes

Webvpn context configuration (config-webvpn-context)
Webvpn group policy configuration (config-webvpn-group)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Entering this command places the router in webvpn URL list configuration mode. In this mode, the list of CIFS server URLs is configured. A URL list can be configured under the SSL VPN context configuration and then separately for each individual policy group configuration. Individual CIFS server URL list configurations must have unique names.

Examples

The following example shows that CIFS URL lists have been added under the webvpn context and for a policy group:

```
webvpn context context1
 ssl authenticate verify all
 !
 acl "acl1"
   error-msg "warning!!!..."
   permit url "http://www.exampleurl1.com"
   deny url "http://www.exampleurl2.com"
   permit http any any
 !
 nbns-list l1
   nbns-server 10.1.1.20
 !
 cifs-url-list "c1"
```

```
  heading "cifs-url"
  url-text "SSLVPN-SERVER2" url-value "\\SSLVPN-SERVER2"
  url-text "SSL-SERVER2" url-value "\\SSL-SERVER2"
!
policy group default
  acl "acl1"
  cifs-url-list "c1"
  nbns-list "l1"
  functions file-access
  functions file-browse
  functions file-entry
default-group-policy default
gateway public
inservice
```

Related Commands

Command	Description
heading	Configures the heading that is displayed above URLs listed on the portal page of a SSL VPN website.
policy group	Attaches a URL list to policy group configuration.
url-text	Adds an entry to a URL list.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

cipherkey

To specify the symmetric keyname that is used to decrypt the filter, use the **cipherkey** command in FPM match encryption filter configuration mode.

cipherkey *keyname*

Syntax Description

keyname	String that is used to decrypt the filter. The value that can be used is realm-etcdf-01.sym.

Command Default

No symmetric keyname is specified.

Command Modes

FPM match encryption filter configuration (c-map-match-enc-config)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

If you have access to an encrypted traffic classification definition file (eTCDF) or if you know valid values to configure encrypted Flexible Packet Matching (FPM) filters, you can configure the same eTCDF through the command-line interface instead of using the preferred method of loading the eTCDF on the router. You must create a class map of type access-control using the **class-map type** command, and use the **match encrypted** command to configure the match criteria for the class map on the basis of encrypted FPM filters and enter FPM match encryption filter configuration mode. You can then use the appropriate commands to specify the algorithm, cipher key, cipher value, filter hash, filter ID, and filter version. You can copy the values from the eTCDF by opening the eTCDF in any text editor.

Use the **cipherkey** command to specify the the symmetric keyname that is used to decrypt the filter.

Examples

The following example shows how to configure the cipherkey for filter decryption:

```
Router(config)# class-map type access-control match-all c1
Router(config-cmap)# match encrypted
Router(c-map-match-enc-config)# cipherkey realm-abc.sym
Router(c-map-match-enc-config)#
```

Related Commands

Command	Description
class-map type	Creates a class map to be used for matching packets to a specified class.
match encrypted	Configures the match criteria for a class map on the basis of encrypted FPM filters and enters FPM match encryption filter configuration mode.

ciphervalue

To specify the encrypted filter contents, use the **ciphervalue** command in FPM match encryption filter configuration mode.

ciphervalue *contents*

Syntax Description

contents	The encrypted filter contents in the format c encrypted-filter-contents c, where c is any delimiting character except + (plus sign), = (equals sign), and / (forward slash).

Command Default

No filter content is specified.

Command Modes

FPM match encryption filter configuration (c-map-match-enc-config)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

If you have access to an encrypted traffic classification definition file (eTCDF) or if you know valid values to configure encrypted Flexible Packet Matching (FPM) filters, you can configure the same eTCDF through the command-line interface instead of using the preferred method of loading the eTCDF on the router. You must create a class map of type access-control using the **class-map type** command, and use the **match encrypted** command to configure the match criteria for the class map on the basis of encrypted FPM filters and enter FPM match encryption filter configuration mode. You can then use the appropriate commands to specify the algorithm, cipher key, cipher value, filter hash, filter ID, and filter version. You can copy the values from the eTCDF by opening the eTCDF in any text editor.

Use the **ciphervalue** command to specify the encrypted filter contents. You can enter up to 200 characters at a time in a multiline input mode for the encrypted filter contents. The new line character (\n) and line feed character (\r) entered in the multiline input mode are ignored in the final cipher value contents.

Examples

The following example shows how to specify the encrypted filter contents:

```
Router(config)# class-map type access-control match-all c1
Router(config-cmap)# match encrypted
Router(c-map-match-enc-config)# ciphervalue #2bcXhFL8Ld1v+DqU+dnxgmONCxl4JrYfcLl95xg
ET0b2B1z0sjoCkozE8YxiH/SXL+eG2wf3ogaA7/Fh
awIH7OF3tUcS5Jwim/u95Xlzh2RLNw819tuIBCdorV
Cu0ZzWCF3vqwpGQzaxtSE4sFgPAvSE2LxZc/VT22
F7EQKBhRo=#
Router(c-map-match-enc-config)#
```

Related Commands

Command	Description
class-map type	Creates a class map to be used for matching packets to a specified class.
match encrypted	Configures the match criteria for a class map on the basis of encrypted FPM filters and enters FPM match encryption filter configuration mode.

cisco (ips-auto-update)

To enable automatic Cisco IOS Intrusion Prevention System (IPS) signature updates from Cisco.com, use the **cisco** command in IPS-auto-update configuration mode. To disable automatic IPS signature updates from Cisco.com, use the **no** form of this command.

cisco

no cisco

Syntax Description

This command has no arguments or keywords.

Command Default

Automatic IPS signature updates from Cisco.com are not enabled.

Command Modes

IPS-auto-update configuration (config-ips-auto-update)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

The **cisco** command cannot be used in conjunction with the **url** command.

Examples

The following example shows how to configure automatic signature updates from Cisco.com that occur at the third hour of the 5 day of the month, at the 56th minute of this hour.

Note Adjustments are made for months without 31 days and daylight savings time.

```
Router(config)# ip ips auto-update
Router(config-ips-auto-update)# cisco
Router(config-ips-auto-update)# occur-at monthly 5 56 3
```

Related Commands

Command	Description
ip ips auto-update	Enables automatic signature updates for Cisco IOS IPS.
occur-at	Defines a preset time for which the Cisco IOS Intrusion Prevention System (IPS) automatically obtains updated signature information.

citrix enabled

To enable Citrix application support for end users in a policy group, use the **citrix enabled** command in webvpn group policy configuration mode. To remove Citrix support from the policy group configuration, use the **no** form of this command.

citrix enabled

no citrix enabled

Syntax Description

This command has no arguments or keywords.

Command Default

Citrix application support is not enabled.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Citrix support allows a citrix client to use applications running on a remote server as if they were running locally. Entering the **citrix-enabled** command configures Citrix support for the policy group.

Examples

The following example configures Citrix support under the policy group:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# citrix enabled
Router(config-webvpn-group)#
```

Related Commands

Command	Description
filter citrix	Configures a Citrix application access filter.
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

class type inspect

To specify the traffic (class) on which an action is to be performed, use the **class type inspect** command in policy-map configuration mode. To delete a class, use the **no** form of this command.

class type inspect *class-map-name*

no class type inspect *class-map-name*

Layer 7 (Application-Specific) Traffic Class Syntax

class type inspect *protocol-name class-map-name*

no class type inspect *protocol-name class-map-name*

Syntax Description

class-map-name	Name of the class on which an action is to be performed. The *class-map-name* must match the appropriate class name specified via the **class-map type inspect** command.
protocol-name	Layer 7 application-specific traffic class. The supported protocols are as follows: • **aol**—America Online Instant Messenger (IM) • **edonkey**—eDonkey peer-to-peer (P2P) • **fasttrack**—FastTrack traffic P2P • **gnutella**—Gnutella Version 2 traffic P2P • **h323** —H.323 protocol, Version 4 • **http**—HTTP • **icq**—I Seek You (ICQ) IM protocol • **imap**—Internet Message Access Protocol (IMAP) • **kazaa2**—Kazaa Version 2 P2P protocol • **msnmsgr**—MSN Messenger IM protocol • **pop3**—Post Office Protocol, Version 3 (POP3) • **sip**—Session Initiation Protocol (SIP) • **smtp**—Simple Mail Transfer Protocol (SMTP) • **sunrpc**—SUN Remote Procedure Call (SUNRPC) • **winmsgr**—Windows Messenger IM protocol • **ymsgr**—Yahoo IM

Command Default

None

Command Modes

Policy-map configuration (config-pmap)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(9)T	Support for the IM protocol and following keywords was added: **aol**, **msnmsgr**, **ymsgr** Support for the P2P protocol and following keywords was added: **edonkey**, **fasttrack**, **gnutella**, **kazaa2**
12.4(20)T	Support for the ICQ and Windows Messenger IM protocols and following keywords was added: **icq**, **winmsgr** Support for the H.323 protocol and following keyword was added: **h323** Support for SIP and following keyword was added: **sip**

Usage Guidelines

Use the **class type inspect** command to specify the class and protocol (if applicable) on which an action is to be performed.

Thereafter, you can specify any of the following actions: drop, inspect, pass, reset, urlfilter, or attach a Layer 7 (application-specific) policy-map to a "top-level" (Layer 3 or Layer 4) policy-map (via the **service-policy (policy-map)** command).

Note A Layer 7 policy is considered to be a nested policy of the top-level policy, and it is called a child policy.

Examples

The following example shows how to configure the policy-map "my-im-pmap" with two IM classes—AOL and Yahoo Messenger—and only allow text-chat messages to pass through. When any packet with a service other than "text-chat" is seen, the connection will be reset.

```
class-map type inspect aol match-any my-aol-cmap
 match service text-chat
!
class-map type inspect ymsgr match-any my-ysmgr-cmap
 match service any
!
policy-map type inspect im my-im-pmap
 class type inspect aol my-aol-cmap
 allow
 log
!
 class type inspect ymsgr my-ysmgr-cmap
 rest
 log
```

Related Commands

Command	Description
class-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect type class map.
policy-map type inspect	Creates a Layer 3 and Layer 4 a or Layer 7 (application-specific) inspect type policy map.
service-policy (policy-map)	Attaches a Layer 7 policy map to a top-level Layer 3 or Layer 4 policy map.

class type urlfilter

To associate a URL filter class with a URL filtering policy map, use the **class type urlfilter** command in policy-map configuration mode. To disassociate the class, use the **no** form of this command.

class type urlfilter [trend | n2h2 | websense] *class-map-name*

no class type urlfilter [trend | n2h2 | websense] *class-map-name*

Syntax Description

trend	(Optional) Specifies that the class map applies to a Trend Micro filtering URL filtering policy. If a keyword is not specified, the class map applies to a local filtering policy.
n2h2	(Optional) Specifies that the class map applies to a SmartFilter URL filtering policy. If a keyword is not specified, the class map applies to a local filtering policy.
websense	(Optional) Specifies that the class map applies to a Websense URL filtering policy. If a keyword is not specified, the class map applies to a local filtering policy.
class-map-name	Name of the URL filter class map.

Command Default

No class is associated with a policy map.

Command Modes

Policy-map configuration (config-pmap)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **class type urlfilter** command to associate a class with a URL filtering policy map. You can associate one or more classes with the URL filtering policy map. You must create the class map for the class before you can associate the class with the policy map. In addition, you must use the **parameter type urlfpolicy** command to associate URL filtering parameters with the policy before you can associate a class with the URL filtering policy map.

Examples

The following example shows how the **class type urlfilter** command is used to create the URL filtering policy map trend-policy and associate three classes with the policy map—trusted-domain-class, untrusted-domain-class, and drop-category.

```
policy-map type inspect urlfilter trend-policy
 parameter type urlfpolicy trend trend-param-map
 class type urlfilter trusted-domain-class
  log
  allow
 class type urlfilter untrusted-domain-class
```

```
 log
 reset
class type urlfilter trend drop-category
 log
 reset
```

Related Commands

Command	Description
policy-map type inspect urlfilter	Creates or modifies a URL filter type inspect policy map.

class-map type inspect

To create a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect type class map, use the **class-map type inspect** command in global configuration mode. To remove a class map from the router configuration file, use the **no** form of this command.

Layer 3 and Layer 4 (Top Level) Class Map Syntax

class-map type inspect {**match-any** | **match-all**} *class-map-name*

no class-map type inspect {**match-any** | **match-all**} *class-map-name*

Layer 7 (Application-Specific) Class Map Syntax

class-map type inspect *protocol-name* {**match-any** | **match-all**} *class-map-name*

no class-map type inspect *protocol-name* {**match-any** | **match-all**} *class-map-name*

Syntax Description

match-any	Determines how packets are evaluated when multiple match criteria exist. Packets must meet one of the match criteria to be considered a member of the class.
match-all	Determines how packets are evaluated when multiple match criteria exist. Packets must meet all of the match criteria to be considered a member of the class. **Note** The **match-all** keyword is available only with Layer 3, Layer 4, and HTTP type class maps.

class-map-name	Name of the class map. The name can be a maximum of 40 alphanumeric characters. The class map name is used to configure policy for the class in the policy map.
protocol-name	Layer 7 application-specific class map. The supported protocols are as follows: • **aol**—America Online Instant Messenger (IM) • **edonkey**—eDonkey peer-to-peer (P2P) • **fasttrack**—FastTrack traffic P2P • **gnutella**—Gnutella Version 2 traffic P2P • **h323**—h323 Protocol, Version 4 • **http**—HTTP • **icq**—I Seek You (ICQ) IM • **imap**—Internet Message Access Protocol (IMAP) • **kazaa2**—Kazaa Version 2 P2P • **msnmsgr**—MSN Messenger IM protocol • **pop3**—Post Office Protocol, Version 3 (POP 3) • **sip**—Session Initiation Protocol (SIP) • **smtp**—Simple Mail Transfer Protocol (SMTP) • **sunrpc**—SUN Remote Procedure Call (SUNRPC) • **winmsgr**—Windows IM • **ymsgr**—Yahoo IM

Defaults

The behavior of the **match-any** keyword is the default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(9)T	The following P2P protocol keywords were added: **edonkey**, **fasttrack**, **gnutella**, **kazaa2**. The following IM protocol keywords were added: **aol**, **msnmsgr**, **ymsgr**.
12.4(15)XZ	This command was integrated into Cisco IOS Release 12.4(15)XZ. Support for the SPA Interface Processor (SIP) protocol was added.
12.4(20)T	The following IM protocol keywords were added: **icq, winmsgr**. The following VoIP protocol keyword was added: **h323** (Version 4).

Usage Guidelines

Use the **class-map type inspect** command to specify the name and protocol (if applicable) of a Layer 3, Layer 4, or Layer 7 class map.

Layer 3 and Layer 4 (Top Level) Class Maps

You can configure a top-level (Layer 3 or Layer 4) class map, which allows you to identify the traffic stream at a high level, by issuing the **match access-group** and **match protocol** commands. These class maps cannot be used to classify traffic at the application level (the Layer 7 level).

Layer 7 (Application-Specific) Class Maps

Application-specific class maps allow you to identify traffic based on the attributes of a given protocol. Match conditions in these class maps are specific to an application (for example, HTTP or SMTP). In addition to the type inspect, you must specify a protocol name (via the *protocol-name* argument) to create an application-specific class map.

Note Configuring the **match access-group** 101 filter enables Layer-4 inspection. As a result, Layer-7 inspection is skipped unless the class-map is of type **match-all**.

Examples

The following example shows how to configure class map c1 with the match criterion of ACL 101 based on the HTTP protocol:

```
class-map type inspect match-all c1
 match access-group 101
 match protocol http
```

The following example configures class map winmsgr-textchat with the match criterion of text-chat based on the Windows IM protocol:

```
class-map type inspect match-any winmsgr winmsgr-textchat
 match service text-chat
```

Related Commands

Command	Description
match access-group	Configures the match criteria for a class map based on the specified ACL number or name.
match class-map	Uses a traffic class as a classification policy.
match protocol	Configures the match criteria for a class map based on the specified protocol.
match service	Configures the match criteria for a class map based on the specified IM protocol.

class-map type urlfilter

To create or modify a URL filter class map, use the **class-map type urlfilter** command in global configuration mode. To remove the class map, use the **no** form of this command.

class-map type urlfilter [**trend | n2h2 | websense**] [**match-any**] *class-map-name*

no class-map type urlfilter [**trend | n2h2 | websense**] [**match-any**] *class-map-name*

Syntax Description

trend	(Optional) Specifies that the class map applies to a Trend Micro URL filtering policy. If a keyword is not specified, the class map applies to a local URL filtering policy.
n2h2	(Optional) Specifies that the class map applies to a SmartFilter URL filtering policy. If a keyword is not specified, the class map applies to a local URL filtering policy.
websense	(Optional) Specifies that the class map applies to a Websense URL filtering policy. If a keyword is not specified, the class map applies to a local URL filtering policy.
match-any	(Optional) Specifies how URL requests are evaluated when multiple match criteria exist in a class map.
class-map-name	Name of the URL filter class map.

Command Default

No class maps are created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **class-map type urlfilter** command to enter class-map configuration mode and create or modify a URL filter class map. The class map is used as a traffic filter to segregate HTTP traffic for which a URL filtering policy applies. If you specify multiple match criteria and want to segregate the traffic when there is at least one match, use the **match-any** keyword. If you do not specify a type of filtering policy with the **trend**, **n2h2**, or **websense** keyword, then the class map applies to a local URL filtering policy.

Local Class Maps

Use the **class-map type urlfilter match-any** *class-map-name* to create or modify a local class map. filtering mode. Typically, you create three local class maps: one to specify trusted domains, one to specify untrusted domains, and one to specify keywords to block.

To specify the match criteria for the trusted and untrusted domain classes, use the following command:

- **match server-domain urlf-glob** *parameter-map-name*

Before you use this command, you must configure the **urlf-glob** parameter with the **parameter-map type urlf-glob** command.

To specify the match criteria for the keyword class map use the following command:

- **match url-keyword urlf-glob** *parameter-map-name*

Before you use this command, you must configure the **urlf-glob** keyword with the **parameter-map type urlf-glob** command.

Trend Micro Class Maps

Use the **class-map type urlfilter trend match-any** *class-map-name* command to create or modify a URL class map for the Trend Router Provisioning Server (TRPS). Typically, you create two Trend Micro class maps: one to specify URL categories and one to specify URL reputations.

To specify the Trend Micro URL categories for which filtering takes place, use the following command:

- **match url category** *category-name*

To specify the Trend Micro URL reputations for which filtering takes place, use the following command:

- **match url reputation** *reputation-name*

SmartFilter Class Maps

Use the **class-map type urlfilter n2h2** *class-map-name* command to create or modify a URL filter class map for a SmartFilter filtering service. Use the following command to specify the match condition for the class map:

- **match server-response any**

Websense Class Maps

Use the **class-map type urlfilter websense** *class-map-name* command to create or modify a URL filter class map for a Websense filtering server. Use the following command to specify the match condition for the class map:

- **match server-response any**

Examples

The following example configures the parameters for local filtering, and then specifies three class maps for local URL filtering: trusted-domain-class, untrusted-domain-class, and keyword-class:

```
parameter-map type urlf-glob trusted-domains-param
 pattern www.example.com
 pattern *.example1.com

parameter-map type urlf-glob untrusted-domain-param
 pattern www.example2.com
 pattern www.example3.org

parameter-map type urlf-glob keyword-param
 pattern games
 pattern adult

class-map type urlfilter match-any trusted-domain-class
 match server-domain urlf-glob trusted-domain-param

class-map type urlfilter match-any untrusted-domain-class
 match server-domain urlf-glob untrusted-domain-param

class-map type urlfilter match-any keyword-class
 match url-keyword urlf-glob keyword-param
```

The following example configures two class maps for Trend Micro filtering: drop-category and drop-reputation:

```
class-map type urlfilter trend match-any drop-category
 match url category Gambling
 match url category Personals-Dating

class-map type urlfilter trend match-any drop-reputation
 match url reputation PHISHING
 match url reputation ADWARE
```

The following example specifies a class map for SmartFilter filtering called n2h2-class and configures the match criteria as any response from the SmartFilter server:

```
class-map type urlfilter n2h2 match-any n2h2-class
 match server-response any
```

Related Commands

Command	Description
match server-domain urlf-glob	Specifies the server domain match criteria for a URL filtering class map.
match server-response any	Specifies the match criterion for SmartFilter and Websense class maps.
match url category	Specifies the URL category match criteria for a URL filtering class map.
match url-keyword urlf-glob	Specifies the URL keyword match criteria for a URL filtering class map.
match url reputation	Specifies the URL reputation match criteria for a URL filtering class map.
parameter-map type urlf-glob	Specifies the filtering parameters for trusted domains, untrusted domains, and blocked keywords.

clear aaa cache filterserver acl

To clear the cache status for a particular filter or all filters, use the **clear aaa cache filterserver acl** command in EXEC mode.

clear aaa cache filterserver acl [*filter-name*]

Syntax Description

filter-name	(Optional) Cache status of a specified filter is cleared.

Command Modes

EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
122(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

After you clear the cache status for a particular filter or all filters, it is recommended that you enable the **show aaa cache filterserver** command to verify that the cache status.

Examples

The following example shows how to clear the cache for all filters:

```
clear aaa cache filterserver acl
```

Related Commands

Command	Description
show aaa cache filterserver	Displays the cache status.

clear aaa cache filterserver group

To clear contents of the server group cache, use the **clear aaa cache filterserver group** command in privileged EXEC mode.

clear aaa cache filterserver group *name*{**all** | **profile** *name*}

Syntax Description

name	Name of the server group being cleared.
all	Clears all profiles.
profile *name*	Clears an individual profile.

Command Default

All profiles are cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following example shows how to clear all RADIUS server IDs:

```
Router# clear aaa cache filterserver group group1
```

Related Commands

Command	Description
aaa cache filterserver	Enables AAA filter server definitions.

clear aaa cache group

To clear an individual entry or all entries in the cache, use the **clear aaa cache group** command in privileged EXEC mode.

clear aaa cache group *name* {**profile** *name* | **all**}

Syntax Description

name	Text string representing the name of a cache server group.
profile *name*	Specifies the name of an individual profile entry to clear.
all	Specifies that all profiles in the named cache group are cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use this command to clear cache entries.

Note To update an old record with profile cache settings and to remove an old record from the cache, clear the cache for the profile.

Examples

The following example clears all cache entries in the localusers group:

```
Router# clear aaa cache group localusers all
```

Related Commands

Command	Description
show aaa cache group	Displays all of the cache entries stored by the AAA cache.

clear aaa counters servers

To clear the authentication, authorization, and accounting (AAA) server information, use the **clear aaa counters servers** command in privileged EXEC mode.

clear aaa counters servers {**all** | **radius** {*server-id* | **all**} | **sg** *name*}

Syntax Description

all	Clears all server information.
radius	Clears RADIUS server information.
server-id	Clears all server IDs displayed by **show aaa servers** command. The range is from 0 to 2147483647.
all	Clears all server IDs.
sg	Clear all servers in a server group.
name	Server group name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release2 .1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following example shows how to clear AAA counter server information:

```
Router# clear aaa counters servers all
```

Related Commands

Command	Description
aaa cache filterserver	Enables AAA filter server definitions.

clear aaa local user fail-attempts

To clear the unsuccessful login attempts of a user, use the **clear aaa local user fail-attempts** command in privileged EXEC mode.

clear aaa local user fail-attempts {**username** *username* | **all**}

Syntax Description

username *username*	Specifies the name of the user.
all	Clears unsuccessful login attempts for all users.

Defaults

Unsuccessful login attempts are not cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

This command is available only to users having the root privilege.

Examples

The following example shows that the unsuccessful login attempts for all users will be cleared:

```
Router# clear aaa local user fail-attempts all
```

Related Commands

Command	Description
aaa local authentication attempts max-fail	Specifies the maximum number of unsuccessful authentication attempts before a user is locked out.
clear aaa local user lockout	Unlocks the locked-out users.
show aaa local user locked	Displays a list of all locked-out users.

clear aaa local user lockout

To unlock the locked-out users, use the **clear aaa local user lockout** command in privileged EXEC mode.

clear aaa local user lockout {**username** *username* | **all**}

Syntax Description

username *username*	Specifies the name of the user to be unlocked.
all	Specifies that all users are to be unlocked.

Defaults

Locked-out users remain locked out.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Only a user having the root privilege can use this command.

Examples

The following example shows that all locked-out users will be unlocked:

```
Router# clear aaa local user lockout all
```

Related Commands

Command	Description
aaa local authentication attempts max-fail	Specifies the maximum number of unsuccessful authentication attempts before a user is locked out.
clear aaa local user fail-attempts	Clears the unsuccessful login attempts of a user.
show aaa local user loced	Displays a list of all locked-out users.

clear access-list counters

To clear the counters of an access list, use the **clear access-list counters** command in privileged EXEC mode.

clear access-list counters {*access-list-number* | *access-list-name*}

Syntax Description

access-list-number	Access list number of the access list for which to clear the counters.
access-list-name	Name of an IP access list. The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Some access lists keep counters that count the number of packets that pass each line of an access list. The **show access-lists** command displays the counters as a number of matches. Use the **clear access-list counters** command to restart the counters for a particular access list to 0.

Examples

The following example clears the counters for access list 101:

```
Router# clear access-list counters 101
```

Related Commands

Command	Description
show access-lists	Displays the contents of current IP and rate-limit access lists.

clear access-template

To manually clear a temporary access list entry from a dynamic access list, use the **clear access-template** command in privileged EXEC mode.

clear access-template {*access-list-number* | *name*} *template-name* {*source-address source-wildcard-bit* | **any** | **host** {*hostname* | *source-address*}} {*destination-address dest-wildcard-bit* | **any** | **host** {*hostname* | *destination-address*}} [**timeout** *minutes*]

Syntax Description

access-list-number	Number of the dynamic access list. The ranges are from 100 to 199 and from 2000 to 2699.
name	Name of an IP access list. • The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.
template-name	Name of a dynamic access list.
source-address	Source address in a dynamic access list. • All other attributes are inherited from the original access-list entry.
source-wildcard-bit	Source wildcard bits.
any	Specifies any source hostname.
host	Specifies a specific source host.
hostname	Name of the host.
destination-address	Destination address in a dynamic access list. • All other attributes are inherited from the original access-list entry.
dest-wildcard-bit	Destination wildcard bits.
timeout *minutes*	(Optional) Specifies a maximum time limit, in minutes, for each entry within this dynamic list. The range is from 1 to 9999. • This is an absolute time, from creation, that an entry can reside in the list. The default is an infinite time limit and allows an entry to remain permanently.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **any**, **host** *hostname*, and **timeout** *minutes* keywords and arguments were added.

Usage Guidelines

The **clear access-template** command is related to the lock-and-key access feature. It clears any temporary access list entries that match the parameters you define.

Examples

The following example shows how to clear any temporary access list entries with a source of 172.20.1.12 from the dynamic access list named vendor:

```
Router> enable
Router# clear access-template vendor 172.20.1.12 any host 172.20.1.13
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-template	Places a temporary access list entry on a router to which you are connected manually.
show ip accounting	Displays the active accounting or checkpointed database or displays access list violations.

clear appfw dns cache

To clear at least one IP address from the Domain Name System (DNS) cache, use the **clear appfw dns cache** command in privileged EXEC mode.

clear appfw dns cache name *dns-name* [**address** *address*]

Syntax Description

name *dns-name*	DNS name of the IM server as entered in the **server name** command in application firewall policy.
address *address*	(Optional) Deletes a specific IP address from the DNS server cache. If an IP address is not specified, all IP addresses for the *dns-name* are deleted from the DNS server cache.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Resolved IP addresses are never "timed out" and not automatically removed from the DNS cache. Thus, if you find an obsolete IP address in the instant messenger database (DNS cache), you can issue the **clear appfw dns cache** command to remove the IP address and prevent the address from being interpreted by the router as an IM server.

Only one IP address can be deleted at a time. If the deleted IP address appears in the subsequent DNS resolution, the IP address is added to the DNS cache again.

Examples

The following example shows how to clear the IP address "172.16.0.0" from the cache of the DNS server "logon.cat.aol.com":

```
Router# clear appfw dns cache name logon.cat.aol.com address 172.16.0.0
```

Related Commands

Command	Description
server	Configures a set of DNS servers for which the specified instant messenger application will be interacting.

clear ase signatures

Note Effective with Cisco IOS Release 12.4(24), the **clear ase signatures** command is not available in Cisco IOS software.

To remove all Automatic Extraction Signatures (ASEs), use the **clear ase signatures** command in privileged EXEC configuration mode.

clear ase signatures

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(24)	This command was removed.

Usage Guidelines

This command is used to remove all the generated signatures that are displayed in the **show ase signatures** command output.

This command is used on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors.

Examples

The following example output demonstrates the result of removing generated signatures:

```
Router# show ase signatures

Automatic Signature Extraction Detected Signatures
==================================================

Signature Hash: 0x1E4A2076AAEA19B1, Offset: 54, Dest Port: TCP 135,
Signature: 05 00 00 03 10 00 00 00 F0 00 10 00 01 00 00 00 B8 00 00 00 00 00 03 00 01 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
Signature Hash: 0x24EC60FB1CF9A800, Offset: 72, Dest Port: TCP 445,
Signature: 00 00 00 00 00 00 00 00 00 00 00 00 FF FE 00 00 00 00 00 62 00 02 50 43 20 4E
45 54 57 4F 52 4B 20 50 52 4F 47 52 41 4D
Signature Hash: 0x0B0275535FFF480C, Offset: 54, Dest Port: TCP 445,
Signature: 00 00 00 85 FF 53 4D 42 72 00 00 00 00 18 53 C8 00 00 00 00 00 00 00 00 00 00
00 00 00 00 FF FE 00 00 00 00 00 62 00 02

Router# clear ase signatures

Router# show ase signatures

Automatic Signature Extraction Detected Signatures
==================================================
```

Table 17 describes the significant fields shown in the display.

Table 17 clear ase signatures Field Descriptions

Field	Description
Signature Hash	Hash (total) value of the 40-byte pattern, used as a check number for error control
Offset	Offset within the packet where the pattern begins
Dest Port	Layer 4 destination port for packets that contain this pattern
Signature	40 bytes of packet data used to potentially identify a piece of malware

Related Commands

Command	Description
ase collector	Enters the ASE collector server IP address so that the ASE sensor has IP connectivity to the ASE collector.
ase group	Identifies the TIDP group number for the ASE feature.
ase enable	Enables the ASE feature on a specified interface.
ase signature extraction	Enables the ASE feature globally on the router.
debug ase	Provides error, log, messaging, reporting, status, and timer information.
show ase	Shows the ASE run-time status, which includes the TIDP group number.

clear authentication sessions

To clear information about current Auth Manager sessions and force 802.1X clients on all 802.1X-enabled interfaces to initialize or reauthenticate, use the **clear authentication sessions** command in privileged EXEC mode.

Note Effective with Cisco IOS Release 12.2(33)SXI, the **clear authentication session** command replaces the **dot1x intitialize** and **dot1x re-authenticate** commands.

clear authentication sessions [**handle** *handle-id*] [**interface** *type number*] [**mac** *mac-address*] [**method** *method-name*] [**session-id** *session-name*]

Syntax Description

handle *handle-id*	(Optional) Specifies the particular handle for which Auth Manager information is to be displayed.
interface *type number*	(Optional) Specifies a particular interface type and number for which Auth Manager information is to be displayed.
mac *mac-address*	(Optional) Specifies the particular MAC address for which you want to display information.
method *method-name*	(Optional) Specifies the particular authentication method for which Auth Manager information is to be displayed.
session-id *session-name*	(Optional) Clears a particular authentication session by reference to its session ID.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Examples

The following example shows how to use the **clear authentication sessions** command to clear information for all Auth Manager sessions:

```
Switch# clear authentication sessions
```

The following example shows how to use the **clear authentication sessions** command to clear information for the Auth Manager session on a particular interface:

```
Switch# clear authentication sessions interface GigabitEthernet/0/23
```

The following example shows how to use the **clear authentication sessions** command to clear information for the Auth Manager session on a particular MAC address:

```
Switch# clear authentication sessions mac 000e.84af.59bd
```

Related Commands

Command	Description
show authentication sessions	Displays information about current Auth Manager sessions.

clear crypto call admission statistics

To clear the counters that track the number of accepted and rejected Internet Key Exchange (IKE) requests, use the **call admission limit** command in global configuration mode.

clear crypto call admission statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following example sets to zero the number of accepted and rejected IKE requests:

```
Router(config)# clear crypto call admission statistics
```

Related Commands

Command	Description
show crypto call admission statistics	Monitors Crypto CAC statistics.

clear crypto ctcp

To clear all Cisco Tunnel Control Protocol (cTCP) sessions and all Internet Key Exchange (IKE) and IPsec security associations (SAs) that are created on those sessions, use the **clear crypto ctcp** command in privileged EXEC mode.

clear crypto ctcp [**peer** *ip-address*]

no clear crypto ctcp [**peer** *ip-address*]

Syntax Description

peer	(Optional) Clears a specific cTCP peer.
ip-address	(Optional) IP address of the peer to be cleared.

Defaults

cTCP sessions are not cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.

Examples

The following example shows that all cTCP sessions and all IKE and IPsec SAs that are created on those sessions are to be cleared:

```
Router# clear crypto ctcp
```

The following example shows that only cTCP sessions for peer 10.76.235.21 and all IKE and IPsec SAs that are created on those sessions are to be cleared.

```
Router# clear crypto ctcp peer 10.76.235.21
```

Related Commands

Command	Description
crypto ctcp	Configures cTCP encapsulation for Easy VPN.

clear crypto datapath

To clear the counters or error history buffers in an encrypted network, use the **clear crypto datapath** command in privileged EXEC mode.

clear crypto datapath {**ipv4** | **ipv6**} [**error** | **internal** | **punt** | **success**]

Syntax Description

ipv4	Clears all counters in a network using IPv4.
ipv6	Clears all counters in a network using IPv6.
error	(Optional) Clears the error history buffer.
internal	(Optional) Clears the internal event counter.
punt	(Optional) Clears the punt event counter.
success	(Optional) Clears the success event counter.

Command Default

All counters are cleared, unless a keyword is entered to specify one counter.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Use the **clear crypto datapath** command to clear the history buffers or counters associated with an encrypted data path. You must specify the IP version for the network. If you only use the IP version keyword, all counters will be cleared. To clear only a specific counter, enter the keyword for that counter.

Examples

The following example shows how to clear all the counters in a network using IP version 4:

```
Router# clear crypto datapath ipv4
```

This example shows how to clear the success counter only:

```
Router# clear crypto datapath ipv4 success
```

Related Commands

Command	Description
show crypto datapath	Displays the counters associated with an encrypted data path.

clear crypto engine accelerator counter

To reset the statistical and error counters of the hardware accelerator of the router or the IPsec Virtual Private Network (VPN) Shared Port Adapter (SPA) to zero, use the **clear crypto engine accelerator counter** command in privileged EXEC mode.

clear crypto engine accelerator counter

IPsec VPN SPA

clear crypto engine accelerator statistic [**slot** *slot*/*subslot* | **all**] [**detail**]

Syntax Description

slot *slot*/*subslot*	(IPsec VPN SPA only—Optional) Chassis slot number and secondary slot number on the SPA Interface Processor (SIP) where the SPA is installed. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide. Resets platform statistics for the corresponding IPsec VPN SPA to zero. This output will not include network interface controller statistics.
all	(IPsec VPN SPA only—Optional) Resets platform statistics for all IPsec VPN SPAs on the router to zero. This reset will not include network interface controller statistics.
detail	(IPsec VPN SPA only—Optional) Resets platform statistics for the IPsec VPN SPA and network interface controller statistics to zero.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(3)XL	This command was introduced for the Cisco uBR905 cable access router.
12.2(2)XA	Support was added for the Cisco uBR925 cable access router.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented for the AIM-VPN/EPII and AIM-VPN/HPII on the following platforms: Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.
12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.3(4)T	The AIM-VPN/BPII was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA to support the IPsec VPN SPA on Cisco 7600 series routers and Catalyst 6500 series switches.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

No specific usage guidelines apply to the hardware accelerators.

IPsec VPN SPA

Enter the **slot** keyword to reset platform statistics for the corresponding IPsec VPN SPA to zero. This reset will not include network interface controller statistics.

Enter the **all** keyword to reset platform statistics for all IPsec VPN SPAs on the router to zero. This reset will not include network interface controller statistics.

Enter the **detail** keyword to reset both the platform statistics for the IPsec VPN SPA and network interface controller statistics to zero.

Examples

Hardware VPN Module

The following example shows the statistical and error counters of the hardware accelerator being cleared to zero:

```
Router# clear crypto engine accelerator counter
```

IPsec VPN SPA

The following example shows the platform statistics for the IPsec VPN SPA in slot 2, subslot 1 being cleared to zero:

```
Router# clear crypto engine accelerator counter slot 2/1
```

The following example shows the platform statistics for all IPsec VPN SPAs on the router being cleared to zero:

```
Router# clear crypto engine accelerator counter all
```

Related Commands

Command	Description
crypto ca	Defines the parameters for the certification authority used for a session.
crypto cisco	Defines the encryption algorithms and other parameters for a session.
crypto dynamic-map	Creates a dynamic map crypto configuration for a session.
crypto engine accelerator	Enables the use of the onboard hardware accelerator for IPsec encryption.
crypto ipsec	Defines the IPSec security associations and transformation sets.
crypto isakmp	Enables and defines the IKE protocol and its parameters.

Command	Description
crypto key	Generates and exchanges keys for a cryptographic session.
crypto map	Creates and modifies a crypto map for a session.
debug crypto engine accelerator control	Displays each control command as it is given to the crypto engine.
debug crypto engine accelerator packet	Displays information about each packet sent for encryption and decryption.
show crypto engine accelerator ring	Displays the contents of command and transmits rings for the crypto engine.
show crypto engine accelerator sa-database	Displays the active (in-use) entries in the crypto engine SA database.
show crypto engine accelerator statistic	Displays the current run-time statistics and error counters for the crypto engine.
show crypto engine brief	Displays a summary of the configuration information for the crypto engine.
show crypto engine configuration	Displays the version and configuration information for the crypto engine.
show crypto engine connections	Displays a list of the current connections maintained by the crypto engine.

clear crypto gdoi

To clear the state of the current session of a Group Domain of Interpretation (GDOI) group member with the key server, use the **clear crypto gdoi** command in privileged EXEC mode.

clear crypto gdoi [**group** *group-name* | **ks coop counters** | **ks policy** | **replay counter** | **ks members counters**]

Syntax Description

group *group-name*	(Optional) Name of the group.
ks coop counters	(Optional) Clears the counters for the cooperative key server.
ks policy	(Optional) Clears all policies on the key server. **Note** (Configuring this keyword does not trigger the re-election of the key servers.)
replay counter	(Optional) Clears the anti-replay counters.
ks members counters	(Optional) Clear the counters for all GMs on the current key server.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(11)T	The **group** and **replay** keywords and the *group-name* argument were added.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.
15.1(3)T	This command was modified. The **ks members counters** keyword combination was added.

Usage Guidelines

If this command is issued on the group member, the policy of the group member is deleted, and the group member reregisters with the key server.

If this command is issued on the key server, the state on the key server is deleted. If redundancy is configured and this command is issued on the key server, the key server goes back into election mode to elect a new primary key server.

Examples

If the following command is issued on the key server, the state on the key server is cleared. If the command is issued on a group member, the state is cleared for the entire group and a reregistration to the key server is forced.

```
Router# clear crypto gdoi
```

If the following command is issued on the key server, the state of the group that is specified is cleared on the key server. If the command is issued on a group member, the state of the group that is specified is cleared on the group member, and reregistration to the key server is forced.

```
Router# clear crypto gdoi group group1
```

The following command clears the anti-replay counters for the GDOI groups:

```
Router# clear crypto gdoi replay counter
```

The following command clears the counters for the cooperative key server:

```
Router# clear crypto gdoi ks coop counters
```

The following command clears all policy on the key server but does not trigger the re-election of the key servers:

```
Router# clear crypto gdoi ks policy
```

The following command clears all counters for all GMs on the current key server:

```
Router# clear crypto gdoi ks members counters
```

clear crypto gdoi ks cooperative role

To reset the cooperative role of the key server and to initiate the election process on the key server, use the **clear crypto gdoi ks cooperative role** command in privileged EXEC mode.

clear crypto gdoi ks cooperative role

Syntax Description

This command has no arguments or keywords.

Command Default

Cooperative role is not reset.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

If the **clear crypto gdoi ks cooperative role** command is executed on a secondary key server, the election is triggered on that secondary key server although that server would most likely remain a secondary key server because there has been an elected primary key server. However, if the **clear crypto gdoi ks cooperative role** command is executed on the primary key server, the primary key server is reassigned to a secondary role, and as a result, a new election that involves all the key servers is triggered. If the previous primary server has the highest priority (of all the key servers), it again becomes the primary server. If the previous primary server does not have the highest priority, the server having the highest priority is elected as the new primary server.

Examples

The following example shows that the cooperative role of the key server has been reset and that the election process is to be initiated:

```
clear crypto gdoi ks cooperative role
```

Related Commands

Command	Description
clear crypto gdoi	Clears the state of the current session of a group member with the key server.

clear crypto ikev2 sa

To clear the Internet Key Exchange Version 2 (IKEv2) security associations (SA), use the **clear crypto ikev2 sa** command in privileged EXEC mode.

clear crypto ikev2 sa [**local** {*ipv4-address* | *ipv6-address*} | **remote** {*ipv4-address* | *ipv6-address*} | **fvrf** *vrf-name* | **psh** *number*]

Syntax Description

local {*ipv4-address* | *ipv6-address*}	(Optional) Clears the IKEv2 security associations matching the local address.
remote {*ipv4-address* | *ipv6-address*}	(Optional) Clears the IKEv2 security associations matching the remote address.
fvrf *vrf-name*	(Optional) Clears the IKEv2 security associations matching the specified front door virtual routing and forwarding (FVRF) instance.
psh *number*	(Optional) Clears the IKEv2 platform service handler matching the specified connection ID.

Command Default

The security associations are not cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. Support was added for IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to clear an IKEv2 security association and the child security associations.

Examples

The following example shows how to clear the IKEv2 security associations:

```
Router# clear crypto ikev2 sa
```

clear crypto ikev2 stat

To clear the Internet Key Exchange Version 2 (IKEv2) statistics, use the **clear crypto ikev2 stat** command in privileged EXEC mode.

clear crypto ikev2 stat

Syntax Description

This command has no arguments or keywords.

Command Default

The IKEv2 security associations statistics are not cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to clear IKEv2 SA statistics.

Examples

The following example shows the IKEv2 statistics being reset and the output of the command:

```
Router# clear crypto ikev2 stat
Cleared crypto ikev2 statistics
```

clear crypto ipsec client ezvpn

To reset the Cisco Easy VPN remote state machine and bring down the Cisco Easy VPN remote connection on all interfaces or on a given interface (tunnel), use the **clear crypto ipsec client ezvpn** command in privileged EXEC mode. If a tunnel name is specified, only the specified tunnel is cleared.

clear crypto ipsec client ezvpn [*name*]

Syntax Description

name	(Optional) Identifies the IPSec virtual private network (VPN) tunnel to be disconnected or cleared with a unique, arbitrary name. If no name is specified, all existing tunnels are disconnected or cleared.

Defaults

If no tunnel name is specified, all active tunnels on the machine are cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(4)YA	This command was introduced for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(8)YJ	This command was enhanced to specify an IPSec VPN tunnel to be cleared or disconnected for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

The **clear crypto ipsec client ezvpn** command resets the Cisco Easy VPN remote state machine, bringing down the current Cisco Easy VPN remote connection and bringing it back up on the interface. If you specify a tunnel name, only that tunnel is cleared. If no tunnel name is specified, all active tunnels on the machine are cleared.

If the Cisco Easy VPN remote connection for a particular interface is configured for autoconnect, this command also initiates a new Cisco Easy VPN remote connection.

Examples

The following example shows the Cisco Easy VPN remote state machine being reset:

```
Router# clear crypto ipsec client ezvpn
```

Related Commands

Command	Description
crypto ipsec client ezvpn (global)	Creates a Cisco Easy VPN remote configuration.
crypto ipsec client ezvpn (interface)	Assigns a Cisco Easy VPN remote configuration to an interface.

clear crypto isakmp

To clear active Internet Key Exchange (IKE) connections, use the **clear crypto isakmp** command in privileged EXEC mode.

clear crypto isakmp [*connection-id*] [**active** | **standby**]

Syntax Description

connection-id	(Optional) ID of the connection that is to be cleared. If this argument is not used, all existing connections will be cleared.
active	(Optional) Clears only IKE security associations (SAs) in the active state. For each active SA that is cleared, the standby router will be notified to clear the corresponding standby SA.
standby	(Optional) Clears only IKE SAs in the standby (secondary) state. **Note** If the router is in standby mode, the router will immediately resynchronize the standby SAs; thus, it may appear as though the standby SAs were not cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.3(11)T	The **active** and **standby** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Caution If the *connection-id* argument is not used, all existing IKE connections will be cleared when this command is issued.

Examples

The following example clears an IKE connection between two peers connected by interfaces 172.21.114.123 and 172.21.114.67:

```
Router# show crypto isakmp sa

    dst           src          state        conn-id   slot
172.21.114.123 172.21.114.67  QM_IDLE           1       0
209.165.201.1  209.165.201.2  QM_IDLE           8       0

Router# clear crypto isakmp 1
```

```
Router# show crypto isakmp sa

    dst             src          state        conn-id   slot
209.165.201.1  209.165.201.2  QM_IDLE           8       0

Router#
```

Related Commands

Command	Description
show crypto isakmp sa	Displays current IKE SAs.

clear crypto sa

To delete IP Security (IPSec) security associations (SAs), use the **clear crypto sa** command in privileged EXEC mode.

clear crypto sa [**active** | **standby**]

Virtual Routing and Forwarding (VRF) Syntax

clear crypto sa peer [**vrf** *fvrf-name*] *address*

clear crypto sa [**vrf** *ivrf-name*]

Crypto Map Syntax

clear crypto sa map *map-name*

IP Address, Security Protocol Standard, and SPI Syntax

clear crypto sa entry *destination-address protocol spi*

Traffic Counters Syntax

clear crypto sa counters

Syntax Description

active	(Optional) Clears only IPSec SAs that are in the active state.
standby	(Optional) Clears only IPSec SAs that are in the standby state. **Note** If the router is in standby mode, the router will immediately resynchronize the standby SAs; thus, it may appear as though the standby SAs were not cleared.
peer [**vrf** *fvrf-name*] *address*	Deletes any IPSec SAs for the specified peer. The *fvrf-name* argument specifies the front door VRF (FVRF) of the peer address.
vrf *ivrf-name*	(Optional) Clears all IPSec SAs whose inside virtual routing and forwarding (IVRF) is the same as the *ivrf-name*.
map	Deletes any IPSec SAs for the named crypto map set.
map-name	Specifies the name of a crypto map set.
entry	Deletes the IPSec SA with the specified address, protocol, and security parameter index (SPI).
destination-address	Specifies the IP address of the remote peer.
protocol	Specifies either the Encapsulation Security Protocol (ESP) or Authentication Header (AH).
spi	Specifies an SPI (found by displaying the SA database).
counters	Clears the traffic counters maintained for each SA; the **counters** keyword does not clear the SAs themselves.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(15)T	The **vrf** keyword and *fvrf-name* argument for **clear crypto sa peer** were added. The **vrf** keyword and *ivrf-name* argument for **clear crypto sa** were added.
12.3(11)T	The **active** and **standby** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

This command clears (deletes) IPSec SAs.

If the SAs were established via Internet Key Exchange (IKE), they are deleted and future IPSec traffic will require new SAs to be negotiated. (When IKE is used, the IPSec SAs are established only when needed.)

If the SAs are manually established, the SAs are deleted and reinstalled. (When IKE is not used, the IPSec SAs are created as soon as the configuration is completed.)

Note If the **peer**, **map**, **entry**, **counters, active**, or **standby** keywords are not used, all IPSec SAs will be deleted.

- The **peer** keyword deletes any IPSec SAs for the specified peer.
- The **map** keyword deletes any IPSec SAs for the named crypto map set.
- The **entry** keyword deletes the IPSec SA with the specified address, protocol, and SPI.
- The **active** and **standby** keywords delete the IPSec SAs in the active or standby state, respectively.

If any of the above commands cause a particular SA to be deleted, all the "sibling" SAs—that were established during the same IKE negotiation—are deleted as well.

The **counters** keyword simply clears the traffic counters maintained for each SA; it does not clear the SAs themselves.

If you make configuration changes that affect SAs, these changes will not apply to existing SAs but to negotiations for subsequent SAs. You can use the **clear crypto sa** command to restart all SAs so that they will use the most current configuration settings. In the case of manually established SAs, if you make changes that affect SAs you must use the **clear crypto sa** command before the changes take effect.

If the router is processing active IPSec traffic, it is suggested that you clear only the portion of the SA database that is affected by the changes, to avoid causing active IPSec traffic to temporarily fail.

Note that this command clears only IPSec SAs; to clear IKE state, use the **clear crypto isakmp** command.

Examples

The following example clears (and reinitializes if appropriate) all IPSec SAs at the router:

```
clear crypto sa
```

The following example clears (and reinitializes if appropriate) the inbound and outbound IPSec SAs established, along with the SA established for address 10.0.0.1 using the AH protocol with the SPI of 256:

```
clear crypto sa entry 10.0.0.1 AH 256
```

The following example clears all the SAs for VRF VPN1:

```
clear crypto sa vrf vpn1
```

Related Commands

Command	Description
clear crypto isakmp	Clears active IKE connections.

clear crypto session

To delete crypto sessions (IP security [IPsec] and Internet Key Exchange [IKE] security associations [SAs]), use the **clear crypto session** command in privileged EXEC mode.

clear crypto session [**local** {*ipv4-address* | *ipv6-address*} [**port** *local-port*]] [**remote** {*ipv4-address* | *ipv6-address*} [**port** *remote-port*]] | [**fvrf** *vrf-name*] [**ivrf** *vrf-name*] | [**isakmp group** *group-name*] | [**username** *user-name*]]

IPsec and IKE Stateful Failover Syntax

clear crypto session [**active** | **standby**]

Syntax Description

local {*ipv4-address* | *ipv6-address*}	(Optional) Clears crypto sessions for a local crypto endpoint. • The IP address is the IP address of the local crypto endpoint.
port *local-port*	(Optional) IKE port of the local endpoint. The *local-port* value can be 1 through 65535. The default value is 500.
remote {*ipv4-address* | *ipv6-address*}	(Optional) Clears crypto sessions for a remote IKE peer. • The IP address is the IP address of the remote IKE peer.
port *remote-port*	(Optional) IKE port of the remote endpoint to be deleted. The *remote-port* value can be from 1 through 65535. The default value is 500.
fvrf *vrf-name*	(Optional) Specifies the front door virtual routing and forwarding (FVRF) session that is to be cleared.
ivrf *vrf-name*	(Optional) Specifies the inside VRF (IVRF) session that is to be cleared.
isakmp group *group-name*	(Optional) Clears the specified crypto session using the isakmp group.
username *user-name*	(Optional) Clears the crypto session for the specified xauth or pki-aaa username.
active	(Optional) Clears only IPsec and IKE SAs in the active state.
standby	(Optional) Clears only IPsec and IKE SAs in the standby state. **Note** If the router is in standby mode, the router will immediately resynchronize the standby SAs with the active router.

Defaults

All existing sessions will be deleted. The IPsec SAs will be deleted first. Then the IKE SAs are deleted.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.3(11)T	The **active** and **standby** keywords were added.

Release	Modification
12.4(11)T	The **isakmp group** *group-name* and **username** *user-name* keywords and associated arguments were added.
15.1(4)M	This command was modified. Support was added for IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

To clear a specific crypto session or a subset of all the sessions, you need to provide session-specific parameters, such as a local or remote IP address, a local or remote port, an FVRF name, or an IVRF name.

If a local IP address is provided as a parameter when you use the **clear crypto session** command, all the sessions (and their IKE SAs and IPsec SAs) that share the IP address as a local crypto endpoint (IKE local address) will be deleted.

Examples

The following example shows that all crypto sessions will be deleted:

```
Router# clear crypto session
```

The following example shows that the crypto session of the FVRF named “blue” will be deleted:

```
Router# clear crypto session fvrf blue
```

The following example shows that the crypto sessions of the FVRF “blue” and the IVRF session “green” will be deleted:

```
Router# clear crypto session fvrf blue ivrf green
```

The following example shows that the crypto sessions of the local endpoint 10.1.1.1 and remote endpoint 10.2.2.2 will be deleted. The local endpoint port is 5, and the remote endpoint port is 10.

```
Router# clear crypto session local 10.1.1.1 port 5 remote 10.2.2.2 port 10
```

Related Commands

Command	Description
show crypto isakmp peer	Displays peer descriptions.
show crypto session	Displays status information for active crypto sessions in a router.

clear crypto pki benchmarks

To clear Public Key Infrastructure (PKI) benchmarking data and release all memory associated with this data, use the **clear crypto pki benchmarks** command in privileged EXEC mode.

clear crypto pki benchmarks

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Use the **clear crypto pki benchmarks** command to clear all PKI benchmarking data and release all memory associated with this data. PKI benchmarking data is used for IOS PKI performance monitoring and optimization. PKI performance monitoring and optimization is turned on or off by using the **crypto pki benchmark** command.

Examples

The following example shows how to clear PKI benchmarking data:

```
Router# clear crypto pki benchmarks
```

Related Commands

Command	Description
crypto pki benchmark	Starts or stops benchmarking data for PKI performance monitoring and optimization.
show crypto pki benchmarks	Displays benchmarking data for PKI performance monitoring and optimization that was collected.

clear crypto pki crls

To remove the certificate revocation list (CRL) database that determines the validity status of digital certificates presented by encryption peers in a PKI, use the **clear crypto pki crls** command in privileged EXEC mode.

clear crypto pki crls

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

The the **clear crypto pki crls** command removes the CRL database that was configured with the **crypto pki certificate chain** command, which is used to configure a certificate authority (CA).

Related Commands

Command	Description
crypto pki certificate chain	Enters certificate chain configuration mode for a specified CA.

clear dmvpn session

To clear Dynamic Multipoint VPN (DMVPN) sessions, use the **clear dmvpn session** command in privileged EXEC mode.

clear dmvpn session [**interface tunnel** *number* | **peer** {*ipv4-address* | *FQDN-string*} | **vrf** *vrf-name*] [**static**]

Syntax Description

interface	(Optional) Displays DMVPN information based on a specific interface.
tunnel *number*	(Optional) Specifies the tunnel address for the DMVPN peer. The range is from 0 to 2147483647.
peer	(Optional) Specifies a DMVPN peer.
ipv4-address	(Optional) The IPv4 address for the DMVPN peer.
FQDN-string	(Optional) Next hop server (NHS) fully qualified domain name (FQDN) string.
vrf *vrf-name*	(Optional) Clears all Next Hop Resolution Protocol (NHRP) sessions related to the specified virtual routing and forwarding (VRF) configuration.
static	(Optional) Clears all static and dynamic NHRP entries. • You must use the **static** keyword for all NHS FQDN configurations. **Note** If the **static** keyword is not specified, only dynamic NHRP entries are cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.4(20)T	This command was modified. The *ipv6-address* argument was added.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
15.1(2)T	This command was modified. The *FQDN-string* argument was added.

Usage Guidelines

This command clears existing DMVPN sessions based on input parameters.

Examples

The following example shows how to clear all DMVPN sessions, both static and dynamic, for the specified peer nonbroadcast multiple access (NBMA) address:

```
Router# clear dmvpn session peer nbma static
```

The following example shows how to clear all DMVPN sessions, both static and dynamic, for the specified peer FQDN string:

```
Router# clear dmvpn session peer examplehub.example1.com static
```

Related Commands

Command	Description
clear ip nhrp	Clears all dynamic entries from the IPv4 NHRP cache.
clear ipv6 nhrp	Clears all dynamic entries from the IPv6 NHRP cache.

clear dmvpn statistics

To clear Dynamic Multipoint VPN (DMVPN) related counters, use the **clear dmvpn statistics** command in privileged EXEC mode.

clear dmvpn statistics [**peer** {**nbma** | **tunnel**} *ip-address*] [**interface** {**tunnel** *number*}] [**vrf** *vrf-name*]

Syntax Description

peer	(Optional) Specifies a DMVPN peer.
nbma	(Optional) Specifies nonbroadcast mapping access (NBMA).
tunnel	(Optional) Specifies a tunnel.
ip-address	(Optional) Specifies the IP address for the DMVPN peer.
interface	(Optional) Displays DMVPN information based on a specific interface.
tunnel *number*	(Optional) Specifies tunnel address for DMVPN peer.
vrf *vrf-name*	(Optional) Clears all DMVPN counters related to the specified virtual routing forwarding (VRF) configuration.

Command Default

DMVPN counters will not be cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Based on input parameters, DMVPN related session counters will be cleared.

Examples

The following example shows how to clear DMVPN related session counters for the specified tunnel interface:

```
Router# clear dmvpn statistics peer tunnel 192.0.2.3
```

Related Commands

Command	Description
clear dmvpn session	Clears DMVPN sessions.

clear dot1x

To clear 802.1X interface information, use the **clear dot1x** command in privileged EXEC mode.

clear dot1x {**all** | **interface** *interface-name*}

Syntax Description

all	Clears 802.1X information for all interfaces.
interface *interface-name*	Clears 802.1X information for the specified interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)SEE	This command was integrated into Cisco IOS Release 12.2(25)SEE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following configuration shows that 802.1X information will be cleared for all interfaces:

```
Router# clear dot1x all
```

The following configuration shows that 802.1X information will be cleared for the Ethernet 0 interface:

```
Router# clear dot1x interface ethernet 0
```

You can verify that the information was deleted by entering the **show dot1x** command.

Related Commands

Command	Description
debug dot1x	Displays 802.1X debugging information.
identity profile default	Creates an identity profile and enters identity profile configuration mode.
show dot1x	Displays details for an identity profile.

clear eap

To clear Extensible Authentication Protocol (EAP) information on a switch or for a specified port, use the **clear eap** command in privileged EXEC mode.

clear eap [**sessions** [**credentials** *credentials-name* | **interface** *interface-name* | **method** *method-name* | **transport** *transport-name*]]

Syntax Description

sessions	(Optional) Clears EAP sessions on a switch or a specified port.
credentials *credentials-name*	(Optional) Clears EAP credential information for only the specified profile.
interface *interface-name*	(Optional) Clears EAP credential information for only the specified interface.
method *method-name*	(Optional) Clears EAP credential information for only the specified method.
transport *transport-name*	(Optional) Clears EAP credential information for only the specified lower layer.

Command Default

All active EAP sessions are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)SEE	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Usage Guidelines

You can clear all counters by using the **clear eap** command with the **sessions** keyword, or you can clear only the specified information by using the **credentials**, **interface**, **method**, or **transport** keywords.

Examples

The following example shows how to clear all EAP information:

```
Router# clear eap sessions
```

The following example shows how to clear EAP session information for the specified profile:

```
Router# clear eap sessions credentials type1
```

Related Commands

Command	Description
show eap registrations	Displays EAP registration information.
show eap sessions	Displays active EAP session information.

clear eou

To clear all client device entries that are associated with a particular interface or that are on the network access device (NAD), use the **clear eou** command in privileged EXEC mode.

clear eou {**all** | **authentication** {**clientless** | **eap** | **static**} | **interface** {*interface-type*} | **ip** {*ip-address*} | **mac** {*mac-address*} | **posturetoken** {*name*}}

Syntax Description

all	Clears all client device entries.
authentication	Authentication type.
clientless	Authentication type is clientless.
eap	Authentication type is Extensible Authentication Procotol (EAP).
static	Authentication type is static.
interface	Provides information about the interface.
interface-type	Type of interface (see Table 18 for a list of interface types).
ip	Specifies an IP address.
ip-address	IP address of the client device.
mac	Specifies a MAC address.
mac-address	The 48-bit address of the client device.
posturetoken	Posture token name.
name	Name of the posture token.

Command Modes

Privileged EXEC#

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Table 18 lists the interface types that may be used for the *interface-type* argument.

Table 18 Description of Interface Types

Interface Type	Description
Async	Asynchronous interface
BVI	Bridge-Group Virtual Interface
CDMA-Ix	Code division multiple access Internet exchange (CDMA Ix) interface
CTunnel	Connectionless Network Protocol (CLNS) tunnel (Ctunnel) interface
Dialer	Dialer interface
Ethernet	IEEE 802.3 standard interface
Lex	Lex interface

Table 18 Description of Interface Types (continued)

Interface Type	Description
Loopback	Loopback interface
MFR	Multilink Frame Relay bundle interface
Multilink	Multilink-group interface
Null	Null interface
Serial	Serial interface
Tunnel	Tunnel interface
Vif	Pragmatic General Multicast (PGM) Multicase Host interface
Virtual-PPP	Virtual PPP interface
Virtual-Template	Virtual template interface
Virtual-TokenRing	Virtual TokenRing interface

Examples

The following example shows that all client device entries are to be cleared:

```
Router# clear eou all
```

Related Commands

Command	Description
eou	Displays information about EAPoUDP.

clear ip access-list counters

To clear IP access list counters, use the **clear ip access-list counters** command in privileged EXEC mode.

clear ip access-list counters [*access-list-number* | *access-list-name*]

Syntax Description

access-list-number | *access-list-name*	(Optional) Number or name of the IP access list for which to clear the counters. If no name or number is specified, all IP access list counters are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

The counter counts the number of packets that match each **permit** or **deny** statement in an access list. You might clear the counters if you want to start at zero to get a more recent count of the packets that are matching an access list. The **show ip access-lists** command displays the counters as a number of matches.

Examples

The following example clears the counter for access list 150:

```
Router# clear ip access-list counters 150
```

Related Commands

Command	Description
show ip access list	Displays the contents of IP access lists.

clear ip access-template

To clear statistical information on the access template, use the **clear ip access-template** command in privileged EXEC mode.

clear ip access-template {*access-list-number* | *name*} *dynamic-name* {*source-address source-wildcard-bit* | **any** | **host** {*hostname* | *source-address*}} {*destination-address dest-wildcard-bit* | **any** | **host** {*hostname* | *destination-address*}}

Syntax Description

access-list-number	Access list number. Range is from 100 to 199 for an IP extended access list and from 2000 to 2699 for an expanded-range IP extended access list.
name	Name of an IP access list. • The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.
dynamic-name	Name of a dynamic access list.
source-address	Source address in a dynamic access list. • All other attributes are inherited from the original access-list entry.
source-wildcard-bit	Source wildcard bits.
any	Specifies any source host name.
host	Specifies a specific source host.
hostname	Name of the host.
destination-address	Destination address in a dynamic access list. • All other attributes are inherited from the original access-list entry.
dest-wildcard-bit	Destination wildcard bits.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **any**, **host** *hostname*, and **timeout** *minutes* keywords and arguments were added.

Examples

This example shows how to clear statistical information on the access list:

```
Router# clear ip access-template 201 list1 any 172.0.2.1 172.0.2.2
```

Related Commands

Command	Description
show mls netflow	Displays configuration information about the NetFlow hardware.

clear ip admission cache

To clear IP admission cache entries from the router, use the **clear ip admission cache** command in privileged EXEC mode.

clear ip admission cache {***** | **host ip address**}

Syntax Description

*****	Clears all IP admission cache entries and associated dynamic access lists.
host ip address	Clears all IP admission cache entries and associated dynamic access lists for the specified host.

Command Modes

Privileged EXEC #

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use this command to clear entries from the admission control cache before they time out.

Examples

The following example shows that all admission entries are to be deleted:

```
Router# clear ip admission cache *
```

The following example shows that the authentication proxy entry for the host with the IP address 192.168.4.5 is to be deleted:

```
Router# clear ip admission cache 192.168.4.5
```

Related Commands

Command	Description
show ip admission cache	Displays the admission control entries or the running admission control configuration.

clear ip audit configuration

To disable Cisco IOS Firewall IDS, remove all intrusion detection configuration entries, and release dynamic resources, use the **clear ip audit configuration** command in EXEC mode.

clear ip audit configuration

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **clear ip audit configuration** EXEC command to disable Cisco IOS Firewall IDS, remove all intrusion detection configuration entries, and release dynamic resources.

Examples

The following example clears the existing IP audit configuration:

```
clear ip audit configuration
```

clear ip audit statistics

To reset statistics on packets analyzed and alarms sent, use the **clear ip audit statistics** command in EXEC mode.

clear ip audit statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **clear ip audit statistics** EXEC command to reset statistics on packets analyzed and alarms sent.

Examples

The following example clears all IP audit statistics:

```
clear ip audit statistics
```

clear ip auth-proxy cache

To clear authentication proxy entries from the router, use the **clear ip auth-proxy cache** command in EXEC mode.

clear ip auth-proxy cache {***** | *host-ip-address*}

Syntax Description

*	Clears all authentication proxy entries, including user profiles and dynamic access lists.
host-ip-address	Clears the authentication proxy entry, including user profiles and dynamic access lists, for the specified host.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to clear entries from the translation table before they time out.

Examples

The following example deletes all authentication proxy entries:

```
clear ip auth-proxy cache *
```

The following example deletes the authentication proxy entry for the host with IP address 192.168.4.5:

```
clear ip auth-proxy cache 192.168.4.5
```

Related Commands

Command	Description
show ip auth-proxy	Displays the authentication proxy entries or the running authentication proxy configuration.

clear ip auth-proxy watch-list

To delete a single watch-list entry or all watch-list entries in Privileged EXEC configuration command mode, use the **clear ip auth-proxy watch-list** command.

clear ip auth-proxy watch-list {*ip-addr* | *****}

Syntax Description

ip-addr	IP address to be deleted from the watch list.
*****	All watch-list entries from the watch list.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is supported on the systems that are configured with a Supervisor Engine 2 only.

If you see entries in the watch list that you suspect are not valid, you can enter the **clear ip auth-proxy watch-list** command to clear them manually instead of waiting for the watch list to expire.

Examples

This example shows how to delete a single watch-list entry:

```
Router# clear ip auth-proxy watch-list 10.0.0.2

Router#
```

This example shows how to delete all watch-list entries:

```
Router# clear ip auth-proxy watch-list *
Router#
```

Related Commands

Command	Description
ip auth-proxy max-login-attempts	Limits the number of login attempts at a firewall interface and QoS filtering and enter the ARP ACL configuration submode.

Command	Description
ip auth-proxy watch-list	Enables and configures an authentication proxy watch list.
show ip auth-proxy watch-list	Displays the information about the authentication proxy watch list.

clear ip inspect ha

To delete the Firewall stateful failover sessions information from a router's memory, use the **clear ip inspect ha** command in privileged EXEC mode.

clear ip inspect ha [sessions all | statistics]

Syntax Description

sessions all	(Optional) Clears all the firewall HA sessions.
statistics	(Optional) Clears the HA statistics on the device.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

If the **clear ip inspect ha sessions all** command is used on the standby device, the standby HA sessions are cleared. This initiates re-synchronization of all HA sessions from the active device to the standby device.

Examples

The following example shows all sessions being deleted:

```
Router# clear ip inspect ha sessions all
```

The following example shows statistics being deleted.

```
Router# clear ip inspect ha statistics
```

clear ip inspect session

To delete Context-Based Access Control (CBAC) configuration and session information from a router's memory, use the **clear ip inspect session** command in privileged EXEC mode.

clear ip inspect session *session-address*

Syntax Description

session-address	Deletes a specific session; the format is 0-FFFFFFFF.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Sessions consist of control channels and data channels.

Use the **clear ip inspect session** command to delete a control channel or a data channel. If you specify a control channel session, then data channel sessions may also be deleted, depending on the application protocols being used. If you specify a data channel session, then only that specific session is deleted.

If you attempt to delete a session and the **clear ip inspect session** command is not supported for the specified protocol, then an error message is generated.

If you want to delete a specific session, use the **show ip inspect session** command to display all session addresses.

Note The **clear ip inspect session** command is recommended for advanced users only because it may disrupt network operations if traffic is still flowing through the session.

Examples

The following example displays the current session addresses:

```
Router# show ip inspect session

Established Sessions

 Session 25A3318 (10.0.0.1:20)=>(10.1.0.1:46068) ftp-data SIS_OPEN

 Session 25A6E1C (10.1.0.1:46065)=>(10.0.0.1:21) ftp SIS_OPEN
```

The following example shows a specific session being deleted:

```
Router# clear ip inspect session 25A6E1C
```

Related Commands

Command	Description
show ip inspect	Displays CBAC configuration and session information.

clear ip ips configuration

To disable Cisco IOS Firewall Intrusion Prevention System (IPS), remove all intrusion detection configuration entries, and release dynamic resources, use the **clear ip ips configuration** command in EXEC mode.

clear ip ips configuration

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	The command name was changed from the **clear ip audit configuration** command to the **clear ip ips configuration** command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example clears the existing IPS configuration:

```
clear ip ips configuration
```

clear ip ips statistics

To reset statistics on packets analyzed and alarms sent, use the **clear ip ips statistics** command in privileged EXEC mode.

clear ip ips statistics [**vrf** *vrf-name*]

Syntax Description

vrf	(Optional) Resets statistics on packets analyzed and alarms sent per VRF.
vrf-name	User specific VRF.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	The command name was changed from the **clear ip audit statistics** command to the **clear ip ips statistics** command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	The **vrf** keyword and argument were added.

Examples

The following example clears all Intrusion Protection System (IPS) statistics:

```
clear ip ips statistics
```

Sample Output for the clear ip ips statistics vrf Command

The following example displays the output of the **clear ip ips statistics vrf** *vrf-name* command:

```
Router# clear ip ips statistics vrf VRF_600
Router# show ip ips statistics vrf VRF_600
Signature statistics [process switch:fast switch]
  signature 5170:1 packets checked: [0:2]
Interfaces configured for ips 3
Session creations since subsystem startup or last reset 0
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [0:0:0]
Last session created 00:02:34
Last statistic reset never
TCP reassembly statistics
  received 8 packets out-of-order; dropped 0
  peak memory usage 12 KB; current usage: 0 KB
  peak queue length 6
```

clear ip sdee

To clear Security Device Event Exchange (SDEE) events or subscriptions, use the **clear ip sdee** command in privileged EXEC mode.

clear ip sdee {**events** | **subscriptions**}

Syntax Description

events	Clears SDEE events from the event buffer.
subscriptions	Clears SDEE subscriptions.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Because subscriptions are properly closed by the Cisco IOS Intrusion Prevention System (IPS) client, this command is typically used only to help with error recovery.

Examples

The following example shows how to clear all open SDEE subscriptions on the router:

```
Router# clear ip sdee subscriptions
```

Related Commands

Command	Description
ip ips notify	Specifies the method of event notification.
ip sdee events	Sets the maximum number of SDEE events that can be stored in the event buffer.
ip sdee subscriptions	Sets the maximum number of SDEE subscriptions that can be open simultaneously.

clear ip trigger-authentication

To clear the list of remote hosts for which automated double authentication has been attempted, use the **clear ip trigger-authentication** command in privileged EXEC mode.

clear ip trigger-authentication

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command when troubleshooting automated double authentication. This command clears the entries in the list of remote hosts displayed by the **show ip trigger-authentication** command.

Examples

The following example clears the remote host table:

```
Router# show ip trigger-authentication

Trigger-authentication Host Table:
Remote Host          Time Stamp
172.21.127.114       2940514234
Router# clear ip trigger-authentication
Router# show ip trigger-authentication
```

Related Commands

Command	Description
show ip trigger-authentication	Displays the list of remote hosts for which automated double authentication has been attempted.

clear ip urlfilter cache

To clear the cache table, use the **clear ip urlfilter cache** command in user EXEC mode.

clear ip urlfilter cache {*ip-address* | **all**} [**vrf** *vrf-name*]

Syntax Description

ip-address	Clears the cache table of a specified server IP address.
all	Clears the cache table completely.
vrf *vrf-name*	(Optional) Clears the cache table only for the specified Virtual Routing and Forwarding (VRF) interface.

Command Modes

User EXEC

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The cache table consists of the most recently requested IP addresses and the respective authorization status for each IP address.

Examples

The following example shows how to clear the cache table of IP address 172.18.139.21:

```
clear ip urlfilter cache 172.18.139.21
```

The following example shows how to clear the cache table of all IP addresses:

```
clear ip urlfilter cache all
```

The following example shows how to clear the cache table of all IP addresses in the vrf named bank.

```
clear ip urlfilter cache all vrf bank
```

Related Commands

Command	Description
ip urlfilter cache	Configures cache parameters.
show ip urlfilter cache	Displays the destination IP addresses that are cached into the cache table.

clear kerberos creds

To delete the contents of the credentials cache, use the **clear kerberos creds** command in privileged EXEC mode.

clear kerberos creds

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Credentials are deleted when this command is issued.

Cisco supports Kerberos 5.

Examples

The following example illustrates the **clear kerberos creds** command:

```
Router# show kerberos creds
Default Principal: chet@cisco.com
Valid Starting          Expires                 Service Principal
18-Dec-1995 16:21:07    19-Dec-1995 00:22:24    krbtgt/CISCO.COM@CISCO.COM

Router# clear kerberos creds
Router# show kerberos creds
No Kerberos credentials.
```

Related Commands

Command	Description
show kerberos creds	Displays the contents of your credentials cache.

clear ldap server

To clear the TCP connection with the Lightweight Directory Access Protocol (LDAP) server, use the **clear ldap server** command in privileged EXEC mode.

clear ldap server *server-name* [**statistics**]

Syntax Description

server-name	LDAP server name.
statistics	(Optional) Clears the statistical information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

Statistics details are not cleared when the server is cleared. To clear the statistics information, use the **statistics** keyword.

Examples

The following example shows how to clear the statistical information:

```
Router# clear ldap server server1 statistics
```

Related Commands

Command	Description
ldap server	Defines an LDAP server and enters LDAP server configuration mode.

clear logging ip access-list cache

To clear all the entries from the Optimized ACL Logging (OAL) cache and send them to the syslog, use the **clear logging ip access-list cache** command in privileged EXEC mode.

clear logging ip access-list cache

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720 only.

Examples

This example shows how to clear all the entries from the OAL cache and send them to the syslog:

```
Router# clear logging ip access-list cache
```

Related Commands

Command	Description
logging ip access-list cache (global configuration)	Configures the OAL parameters globally.
logging ip access-list cache (interface configuration)	Enables an OAL-logging cache on an interface that is based on direction.
show logging ip access-list	Displays information about the logging IP access list.

clear parameter-map type protocol-info

To clear the Domain Name System (DNS) cache for name resolution of servers within a parameter map, use the **clear parameter-map type protocol-info** command in privileged EXEC mode.

clear parameter-map type protocol-info dns-cache *dns-name* [**ip-address** *ip-address]*

Syntax Description

dns-cache *dns-name*	Cache of the specified DNS server will be cleared.
ip-address *ip-address*	(Optional) Specified IP address is removed from the cache of the DNS server. If an IP address is not specified, all IP addresses from the specified DNS server are cleared from the cache.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(9)T	This command was introduced.

Examples

The following example shows how to clear the cache of the DNS server “sdsc.msg.yahoo.com:

```
Router# clear parameter-map type protocol-info dns-cache sdsc.msg.yahoo.com
```

Related Commands

Command	Description
parameter-map type	Creates or modifies a parameter map.

clear policy-firewall

To reset the information collected by the firewall, use the **clear policy-firewall** command in user EXEC or privileged EXEC mode.

clear policy-firewall {**session** [*session address* | **class-map** *class-map-name* | **policy-map** *policy-map-name*] | **stats** [*drop-counters*] | **summary-log** | **zone-pair**}

Syntax Description

session *session address*	Clears the session.
class-map *class-map-name*	Clears the class map.
policy-map *policy-map-name*	Clears the policy map.
stats [*drop-counters*]	Clears the statistics and the drop-counters.
summary-log	Clears the summary log.
zone-pair	Clears the zone-pair.

Command Default

The firewall information is not cleared.

Command Modes

EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

Use this command to clear the information that is collected by the firewall. The cleared counters include drop-counters, summary-log buffers, sessions and zone pairs.

Examples

The following example shows how to clear the zone pair:

```
Router(mode-prompt)# clear policy-firewall zone-pair
```

Related Commands

Command	Description
show policy-firewall config	Displays the entire configuration of the firewall in the router.
show policy-firewall sessions	Displays the details of the firewall sessions.

Command	Description
show policy-firewall stats	Displays the statistics of all firewall activities in the router.
show policy-firewall summary-log	Displays the summary log of the firewall.

clear policy-firewall stats vrf

To clear the policy firewall statistics at a VPN Routing and Forwarding (VRF) level, use the **clear policy-firewall stats vrf** command in privileged EXEC mode.

clear policy-firewall stats vrf *vrf-name*

Syntax Description

vrf-name	Name of the VRF.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Examples

The following example shows how to clear the configured policy firewall VRF statistics:

```
Router# clear policy-firewall stats vrf vrf1
```

Related Commands

Command	Description
show policy-firewall stats vrf	Displays VRF-level policy firewall statistics.

clear policy-firewall stats vrf global

To clear the global VPN Routing and Forwarding (VRF) policy firewall statistics, use the **clear policy-firewall stats vrf global** command in privileged EXEC mode.

clear policy-firewall stats vrf global

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Examples

The following example shows how to clear the global policy firewall statistics:

```
Router# clear policy-firewall stats vrf global
```

Related Commands

Command	Description
show policy-firewall stats vrf global	Displays information about the global VRF firewall policies.

clear policy-firewall stats zone

To clear the policy firewall statistics at a zone level, use the **clear policy-firewall stats zone** command in privileged EXEC mode.

clear policy-firewall stats zone *zone-name*

Syntax Description

zone-name	Name of the zone.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Examples

The following example shows how to clear the configured policy firewall zone statistics:

```
Router# clear policy-firewall stats zone zone1
```

Related Commands

Command	Description
show policy-firewall stats zone	Displays policy firewall statistics at a zone level.

clear port-security

To delete configured secure MAC addresses and sticky MAC addresses from the MAC address table in the Privileged EXEC configuration command mode, use the **clear port-security** command.

clear port-security dynamic [**address** *mac-addr* | **interface** *interface-id*] [**vlan** *vlan-id*]

Syntax Description

address *mac-addr*	(Optional) Deletes the specified secure MAC address or sticky MAC address.
interface *interface-id*	(Optional) Deletes all secure MAC addresses and sticky MAC addresses on the specified physical port or port channel.
vlan *vlan-id*	(Optional) Deletes the specified secure MAC address or sticky MAC address from the specified VLAN.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	The output of this command was changed to support sticky MAC addresses on the Supervisor Engine 720 only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on negotiated trunks only.

If you enter the **clear port-security** command without adding any keywords or arguments, the switch removes all the secure MAC addresses and sticky MAC addresses from the MAC address table.

If you enter the **clear port-security dynamic interface** *interface-id* command, all the secure MAC addresses and sticky MAC addresses on an interface are removed from the MAC address table.

You can verify that the information was deleted by entering the **show port-security** command.

Examples

This example shows how to remove a specific secure address from the MAC address table:

```
Router# clear port-security dynamic address 0008.0070.0007
Router#
```

This example shows how to remove all the secure MAC addresses and sticky MAC addresses learned on a specific interface:

```
Router# clear port-security dynamic interface gigabitethernet0/1
Router#
```

Related Commands

Command	Description
show port-security	Displays information about the port-security setting.
switchport port-security mac-address	Adds a MAC address to the list of secure MAC addresses.

clear radius

To clear the RADIUS server information, use the **clear radius** command in privileged EXEC mode.

clear radius {**sg-stats** | **statistics**}

Syntax Description

sg-stats	Clears the RADIUS server group statistics.
statistics	Clears the RADIUS statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows how to clear the RADIUS statistics information:

```
Router# clear radius statistics
```

Related Commands

Command	Description
radius-server host	Configures a RADIUS server host.

clear radius local-server

To clear the display on the local server or to unblock a locked username, use the **clear radius local-server** command in privileged EXEC mode.

clear radius local-server {**statistics** | **user** *username*}

Syntax Description

statistics	Clears the display of statistical information.
user	Unblocks the locked username specified.
username	Locked username.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)JA	This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Examples

The following example shows how to unblock the locked username “smith”:

```
Router# clear radius local-server user smith
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.

clear webvpn nbns

To clear the NetBIOS name service (NBNS) cache on a SSL VPN gateway, use the **clear webvpn nbns** command in privileged EXEC mode.

clear webvpn nbns [**context** {*name* | **all**}]

Syntax Description

context	(Optional) Clears NBNS statistics for a specific context or all contexts.
name	Clears NBNS statistics for a specific context.
all	Clears NBNS statistics for all contexts.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Entering this command without any keywords or arguments clears all NBNS counters on the network device.

Examples

The following example clears all NBNS counters:

```
Router# clear webvpn nbns
```

Related Commands

Command	Description
clear webvpn session	Clears remote users sessions on a SSL VPN gateway.
clear webvpn stats	Clears application and access counters on a SSL VPN gateway.

clear webvpn session

To clear SSL VPN remote user sessions, use the **clear webvpn session** command in privileged EXEC mode.

clear webvpn session [**user** *name*] **context** {*name* | **all**}

Syntax Description

user *name*	(Optional) Clears session information for a specific user.
context {*name* | **all**}	Clears session information for a specific context or all contexts.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command is used to clear the session for either the specified remote user or all remote users in the specified context.

Examples

The following example clears all session information:

```
Router# clear webvpn session context all
```

Related Commands

Command	Description
clear webvpn nbns	Clears the NBNS cache on a SSL VPN gateway.
clear webvpn stats	Clears application and access counters on a SSL VPN gateway.

clear webvpn stats

To clear (or reset) SSL VPN application and access counters, use the **clear webvpn stats** command in privileged EXEC mode.

clear webvpn stats [[**cifs** | **citrix** | **mangle** | **port-forward** | **sso** | **tunnel**] [**context** {*name* | **all**}]]

Syntax Description

cifs	(Optional) Clears Windows file share (CIFS) statistics.
citrix	(Optional) Clears Citrix application statistics.
mangle	(Optional) Clears URL mangling statistics.
port-forward	(Optional) Clears port forwarding statistics.
sso	(Optional) Clears statistics for Single SignOn (SSO) activities.
tunnel	(Optional) Clears Cisco AnyConnect VPN Client tunnel statistics.
context {*name* | **all**}	(Optional) Clears information for either a specific context or all contexts.

Command Default

If no keywords are entered, all SSL VPN application and access counters are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(11)T	The **sso** keyword was added.

Usage Guidelines

This command is used to clear counters for Windows file shares, Citrix applications, URL mangling, application port forwarding, SSO, and Cisco AnyConnect VPN Client tunnels. The counters are cleared for either the specified context or all contexts on the SSL VPN gateway.

Examples

The following example clears all statistics counters for all SSL VPN processes:

```
Router# clear webvpn stats
```

The following example clears statistics for SSO activities:

```
Router# clear webvpn stats sso
```

Related Commands

Command	Description
clear webvpn nbns	Clears the NBNS cache on a SSL VPN gateway.
clear webvpn session	Clears remote users sessions on a SSL VPN gateway.

clear zone-pair

To clear the policy map counters, inspect sessions, or the URL filter cache on a zone-pair, use the **clear zone-pair** command in privileged EXEC mode.

clear zone-pair [*zone-pair-name*] {**counter** | **inspect session** | **urlfilter cache**}

Syntax Description

zone-pair-name	(Optional) Name of the zone-pair on which counters, inspect sessions, or the uRL filter cache are cleared.
counter	Clears the policy-map counters. Resets the statistics of the inspect type policy map on the specified zone-pair.
inspect session	Deletes the inspect sessions on the specified zone-pair.
urlfilter cache	Clears the URL filter cache on the specified zone-pair.

Command Default

Disabled (it is not necessary to enter this command).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was implemented on the following platforms: Cisco 881 and Cisco 888.

Usage Guidelines

If you do not specify a zone-pair name, the policy map counters, sessions, or the URL filter cache are cleared for all the configured zone-pairs.

Examples

The following example deletes the inspect sessions on the zp zone-pair:

```
Router# clear zone-pair zp inspect session
```

The following example clears the URL filter cache on the zp zone-pair.

```
Router# clear zone-pair zp urlfilter cache
```

clid

To preauthenticate calls on the basis of the Calling Line IDentification (CLID) number, use the **clid** command in AAA preauthentication configuration mode. To remove the **clid** command from your configuration, use the **no** form of this command.

clid [**if-avail | required**] [**accept-stop**] [**password** *password*]

no clid [**if-avail | required**] [**accept-stop**] [**password** *password*]

Syntax Description

if-avail	(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.
required	(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.
accept-stop	(Optional) Prevents subsequent preauthentication elements such as ctype or dnis from being tried once preauthentication has succeeded for a call element.
password *password*	(Optional) Defines the password for the preauthentication element. The default password string is cisco.

Command Default

The **if-avail** and **required** keywords are mutually exclusive. If the **if-avail** keyword is not configured, the preauthentication setting defaults to **required**.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

You may configure more than one of the authentication, authorization and accounting (AAA) preauthentication commands (**clid**, **ctype**, **dnis**) to set conditions for preauthentication. The sequence of the command configuration decides the sequence of the preauthentication conditions. For example, if you configure **dnis**, then **clid**, then **ctype**, in this order, then this is the order of the conditions considered in the preauthentication process.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

Examples

The following example specifies that incoming calls be preauthenticated on the basis of the CLID number:

```
aaa preauth
 group radius
 clid required
```

Related Commands

Command	Description
ctype	Preauthenticates calls on the basis of the call type.
dnis (RADIUS)	Preauthenticates calls on the basis of the DNIS number.
dnis bypass (AAA preauthentication configuration)	Specifies a group of DNIS numbers that will be bypassed for preauthentication.
group (RADIUS)	Specifies the AAA RADIUS server group to use for preauthentication.

client

To specify a RADIUS client from which a device will accept Change of Authorization (CoA) and disconnect requests, use the **client** command in dynamic authorization local server configuration mode. To remove this specification, use the **no** form of this command.

client {*name* | *ip-address*} [**key** [**0** | **7**] *word*] [**vrf** *vrf-id*]

no client {*name* | *ip-address*} [**key** [**0** | **7**] *word*] [**vrf** *vrf-id*]

Syntax Description

name	Hostname of the RADIUS client.
ip-address	IP address of the RADIUS client.
key	(Optional) Configures the RADIUS key to be shared between a device and a RADIUS client.
0	(Optional) Specifies that an unencrypted key will follow.
7	(Optional) Specifies that a hidden key will follow.
word	(Optional) Unencrypted server key.
vrf *vrf-id*	(Optional) Virtual Routing and Forwarding (VRF) ID of the client.

Command Default

CoA and disconnect requests are dropped.

Command Modes

Dynamic authorization local server configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

A device (such as a router) can be configured to allow an external policy server to dynamically send updates to the router. This functionality is facilitated by the CoA RADIUS extension. CoA introduced peer-to-peer capability to RADIUS, enabling a router and external policy server each to act as a RADIUS client and server. Use the **client** command to specify the RADIUS clients for which the router will act as server.

Examples

The following example configures the router to accept requests from the RADIUS client at IP address 10.0.0.1:

```
aaa server radius dynamic-author
 client 10.0.0.1 key cisco
```

Related Commands

Command	Description
aaa server radius dynamic-author	Configures an ISG as a AAA server to facilitate interaction with an external policy server.

client authentication list

To configure Internet Key Exchange (IKE) extended authentication (Xauth) in an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **client authentication list** command in ISAKMP profile configuration mode. To restore the default behavior, which is that Xauth is not enabled, use the **no** form of this command.

client authentication list *list-name*

no client authentication list *list-name*

Syntax Description

list-name	Character string used to name the list of authentication methods activated when a user logs in. The list name must match the list name that was defined during the authentication, authorization, and accounting (AAA) configuration.

Defaults

No default behaviors or values

Command Modes

ISAKMP profile configuration (config-isakmp-profile)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11.5)	Xauth no longer has to be disabled globally for it to be enabled on a profile basis.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Before configuring Xauth, you must set up an authentication list using AAA commands.

Xauth can be enabled on a profile basis if it has been disabled globally.

Effective with Cisco IOS Release 12.4(11.5), Xauth on either a server or client does not need to be disabled globally to enable it on profile basis.

Examples

The following example shows that user authentication is configured. User authentication is a list of authentication methods called “xauthlist” in an ISAKMP profile called “vpnprofile.”

```
crypto isakmp profile vpnprofile
 client authentication list xauthlist
```

The following example shows that Xauth has been disabled globally and enabled for the profile “nocerts”:

```
no crypto xauth FastEthernet0/0
!
crypto isakmp policy 1
 encr 3des
 group 2
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp client configuration group HRZ

crypto isakmp client configuration group vpngroup
 key cisco123
 pool vpnpool
crypto isakmp profile cert_sig
   match identity group HRZ
   isakmp authorization list isakmpauth
   client configuration address respond
   client configuration group HRZ
crypto isakmp profile nocerts
   match identity group vpngroup
   client authentication list vpn-login
   isakmp authorization list isakmpauth
   client configuration address respond
```

Related Commands

Command	Description
aaa authentication login	Sets AAA authentication at login.

client configuration address

To configure Internet Key Exchange (IKE) configuration mode in the Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **client configuration address** command in ISAKMP profile configuration mode. To disable IKE configuraton mode, use the **no** form of this command.

client configuration address {**initiate** | **respond**}

no client configuration address {**initiate** | **respond**}

Syntax Description

initiate	Router will attempt to set IP addresses for each peer.
respond	Router will accept requests for IP addresses from any requesting peer.

Defaults

IKE configuration is not enabled.

Command Modes

ISAKMP profile configuration (config-isa-prof)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Before you can use this command, you must enter the **crypto isakmp profile** command.

Examples

The following example shows that IKE mode is configured to either initiate or respond in an ISAKMP profile called “vpnprofile”:

```
crypto isakmp profile vpnprofile
 client configuration address initiate
 client configuration address respond
```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile.

client configuration group

To associate a group with the peer that has been assigned an Internet Security Association Key Management Protocol (ISAKMP) profile, use the **client configuration group** command in crypto ISAKMP profile configuration mode. To disable this option, use the **no** form of this command.

client configuration group *group-name*

no client configuration group *group-name*

Syntax Description

group-name	Name of the group to be associated with the peer.

Defaults

No default behavior or values

Command Modes

Crypto ISAKMP profile configuration (conf-isa-prof)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **client configuration group** command is used after the crypto map has been configured and the ISAKMP profiles have been assigned to them.

Examples

The following example shows that the group “some_group” is to be associated with the peer:

```
crypto isakmp profile id_profile
   ca trust-point 2315
   match identity host domain cisco.com
   client configuration group some_group
```

Related Commands

Command	Description
match certificate (ISAKMP)	Assigns an ISAKMP profile to a peer on the basis of the contents of arbitrary fields in the certificate.

client pki authorization list

To specify the authorization list of AAA servers that will be used to obtain per-user AAA attributes on the basis of the username that is constructed from the certificate, use the **client pki authorization list** command in crypto ISAKMP profile configuration mode. To disable the list name, use the **no** form of this command.

client pki authorization list *listname*

no client pki authorization list *listname*

Syntax Description

listname	Definition of the argument needed, including syntax-level defaults, if any.

Command Default

User attributes are not pushed to the remote device.

Command Modes

Crypto ISAKMP profile configuration (config-isakmp-profile)

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

This command is used inside the crypto Internet Security Association and Key Management Protocol (ISAKMP) profile.

Examples

The following example shows that user attributes are to be obtained from the AAA server (list name “usrgrp”) and pushed to the remote device:

```
crypto isakmp profile ISA-PROF
   match certificate CERT-MAP
   isakmp authorization list usrgrp
   client pki authorization list usrgrp
   client configuration address respond
   client configuration group pkiuser
   virtual-template 2
```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile and audits IPsec user sessions.

client rekey encryption

To set the client acceptable rekey ciphers for the key-encryption-key (KEK), use the **client rekey encryption** command in GDOI group configuration mode. To remove the client acceptable rekey ciphers, use the **no** form of this command.

client rekey encryption *cipher* [...[*cipher*]]

no client rekey encryption

Syntax Description

cipher	Any of the following ciphers: • **3des-cbc**—Specifies triple Data Encryption Standard (3DES) in Cipher-block chaining (CBC) mode. • **aes 128**—Specifies 128-bit Advanced Encryption Standard (AES). • **aes 192**—Specifies 192-bit AES. • **aes 256**—Specifies 256-bit AES. • **des-cbc**—Specifies DES in CBC mode.

Command Default

Any cipher assigned by the key server is accepted.

Command Modes

GDOI group configuration (config-gdoi-group)

Command History

Release	Modification
Cisco IOS XE Release 2.4.1	This command was introduced.
Cisco IOS Release 15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

Use the **client rekey encryption** command to specify the acceptable ciphers for KEK. Multiple ciphers can be specified. If a cipher is not set using this command, the cipher assigned by the key server is accepted.

Examples

The following example shows how to set the acceptable ciphers for KEK:

```
Router# configure terminal
Router(config)# crypto gdoi group GETVPN
Router(config-gdoi-group)# identity number 1111
Router(config-gdoi-group)# server address ipv4 192.10.2.10
Router(config-gdoi-group)# client rekey encryption 3des-cbc aes 192 aes 256
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.

client rekey hash

To set acceptable hash algorithms for rekey message signing, use the **client rekey hash** command in GDOI group configuration mode. To remove the acceptable hash algorithms, use the **no** form of this command.

client rekey hash *hash*

no client rekey hash

Syntax Description

hash	Hash for rekey message signing. The supported hash in Cisco IOS XE Release 2.4.1 is Secure Hash Standard (**sha**).

Command Default

Any hash selected by the key server is accepted.

Command Modes

GDOI group configuration (config-gdoi-group)

Command History

Release	Modification
Cisco IOS XE Release 2.4.1	This command was introduced.
Cisco IOS Release 15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

Use the **client rekey hash** command to select the acceptable hash for the rekey message signing. If a hash is not set using this command, the hash selected by the key server is accepted.

Examples

The following example shows how to set the acceptable hash for rekey message signing:

```
Router# configure terminal
Router(config)# crypto gdoi group GETVPN
Router(config-gdoi-group)# identity number 1111
Router(config-gdoi-group)# server address ipv4 192.10.2.10
Router(config-gdoi-group)# client rekey hash sha
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.

client transform-sets

To specify up to 6 acceptable transform-set tags used by the traffic-encryption-key (TEK) for data encryption or authentication, use the **client transform-sets** command in GDOI group configuration mode. To remove the acceptable transform-set tags, use the **no** form of this command.

client transform-sets *transform-set-name1* [... [*transform-set-name6*]]

no client transform-sets

Syntax Description

transform-set-name	Transform-tags used by the TEK for data encryption or authentication.

Command Default

The transform-set selected by the key server is accepted.

Command Modes

GDOI group configuration (config-gdoi-group)

Command History

Release	Modification
Cisco IOS XE Release 2.4.1	This command was introduced.
Cisco IOS Release 15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

Use the **client transform-sets** command to specify up to 6 transform-set tags used by the TEK for data encryption or authentication. If this command is not issued, the transform-set selected by the key server is accepted. The security protocol configured in the transform set must be Encapsulating Security Payload (ESP), which is the only protocol supported by GETVPN in Cisco IOS XE Release 2.4.1.

Examples

The following example shows how to set the transform-set tags used by TEK for data encryption or authentication:

```
Router# configure terminal
Router(config)# crypto ipsec transform-set g1 esp-aes 192 esp-sha-hmac
Router(cfg-crypto-trans)# exit
Router(config)# crypto gdoi group GETVPN
Router(config-gdoi-group)# client transform-sets g1
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
crypto ipsec transform-set	Defines a transform set—an acceptable combination of security protocols and algorithms.

commands (view)

To add commands or an interface to a command-line interface (CLI) view, use the **commands** command in view configuration mode. To delete a command or an interface from a CLI view, use the **no** form of this command.

Syntax for Adding and Deleting Commands to a View

commands *parser-mode* {**include** | **include-exclusive** | **exclude**} [**all**] [*command*]

no commands *parser-mode* {**include** | **include-exclusive** | **exclude**} [**all**] [*command*]

Syntax for Adding and Deleting Interfaces to a View

commands *parser-mode* {**include** | **include-exclusive**} [**all**] [**interface** *name*] [*command*]

no commands *parser-mode* {**include** | **include-exclusive**} [**all**] [**interface** *name*] [*command*]

Syntax Description

parser-mode	Mode in which the specified command exists. See Table 19 in the "Usage Guidelines" section for a list of available options for this argument.
include	Adds a specified command or a specified interface to the view and allows the same command or interface to be added to a view.
include-exclusive	Adds a specified command or a specified interface to the view and excludes the same command or interface from being added to all other views.
exclude	Denies access to commands in the specified parser mode. **Note** This keyword is available only for command-based views.
all	(Optional) A "wildcard" that allows every command in a specified configuration mode that begins with the same keyword or every subinterface within a specified interface to be part of the view.
command	(Optional) Command that is added to the view. **Note** If no commands are specified, all commands within the specified parser mode are included or excluded, as appropriate.
interface *name*	(Optional) Interface that is added to the view.

Defaults

If this command is not enabled, a view will not have adequate information to deny or allow access to users.

Command Modes

View configuration (config-view)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.3(11)T	The **exclude** keyword and the **interface** *interface-name* option were added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

If a network administrator does not enter a specific command (via the *command* argument) or interface (via the **interface** *interface-name* option), users are granted access (via the **include** or **include-exclusive** keyword) or denied access (via the **exclude** keyword) to all commands within the specified parser mode.

parser-mode Options

Table 19 shows some of the keyword options for the *parser-mode* argument in the **commands** command. The available mode keywords vary depending on your hardware and software version. To display a list of available mode options on your system, use the **commands ?** command.

Table 19 parser-mode Argument Options

Command	Description
accept-dialin	VPDN accept-dialin group configuration mode
accept-dialout	VPDN accept-dialout group configuration mode
address-family	Address family configuration mode
alps-ascu	ALPS ASCU configuration mode
alps-circuit	ALPS circuit configuration mode
atm-bm-config	ATM bundle member configuration mode
atm-bundle-config	ATM bundle configuration mode
atm-vc-config	ATM virtual circuit configuration mode
atmsig_e164_table_mode	ATMSIG E164 Table
cascustom	Channel-associated signaling (cas) custom configuration mode
config-rtr-http	RTR HTTP raw request configuration mode
configure	Global configuration mode
controller	Controller configuration mode
crypto-map	Crypto map configuration mode
crypto-transform	Crypto transform configuration mode
dhcp	DHCP pool configuration mode
dspfarm	DSP farm configuration mode
exec	EXEC mode
flow-cache	Flow aggregation cache configuration mode
gateway	Gateway configuration mode

Table 19 parser-mode Argument Options (continued)

Command	Description
interface	Interface configuration mode
interface-dlci	Frame Relay DLCI configuration mode
ipenacl	IP named extended access-list configuration mode
ipsnacl	IP named simple access-list configuration mode
ip-vrf	Configure IP VRF parameters
lane	ATM Lan Emulation Lecs Configuration Table
line	Line configuration mode
map-class	Map-class configuration mode
map-list	Map-list configuration mode
mpoa-client	MPOA client
mpoa-server	MPOA server
null-interface	Null interface configuration mode
preaut	AAA Preauth definitions
request-dialin	VPDN accept-dialin group configuration mode
request-dialout	VPDN accept-dialout group configuration mode
route-map	Route-map configuration mode
router	Router configuration mode
rsvp_policy_local	RSVP local policy configuration mode
rtr	RTR entry configuration mode
sg-radius	RADIUS server group definition
sg-tacacs+	TACACS+ server group
sip-ua	SIP UA configuration mode
subscriber-policy	Subscriber policy configuration mode
tcl	Tcl mode
tdm-conn	TDM connection configuration mode
template	Template configuration mode
translation-rule	Translation Rule configuration mode
vc-class	VC class configuration mode
voiceclass	Voice class configuration mode
voiceport	Voice configuration mode
voipdialpeer	Dial peer configuration mode
vpdn-group	VPDN group configuration mode

Examples

The following example shows how to add the privileged EXEC command **show version** to both CLI views “first” and “second.” Because the **include** keyword was issued, the **show version** command can be added to both views.

```
Router(config)# parser view first
Router(config-view)# secret 5 secret
Router(config-view)# commands exec include show version
!
Router(config)# parser view second
Router(config-view)# secret 5 myview
Router(config-view)# commands exec include show version
```

The following example shows how to allow users in the view “first” to execute all commands that start with the word “show” except the **show interfaces** command, which is excluded by the view “second”:

```
Router(config)# parser view first
Router(config-view)# secret 5 secret
Router(config-view)# commands exec include all show
!
Router(config)# parser view second
Router(config-view)# secret 5 myview
Router(config-view)# commands exec include-exclusive show interfaces
```

Related Commands

Command	Description
parser view	Creates or changes a CLI view and enters view configuration mode.
secret 5	Associates a CLI view or a superview with a password.

configuration url

To specify on a server the URL that an Easy VPN remote device must use to get a configuration in a Mode Configuration Exchange, use the **configuration url** command in global configuration mode. To delete the URL, use the **no** form of this command.

configuration url {*url*}

no configuration url {*url*}

Syntax Description

url	Specifies the URL the Easy VPN remote device must use to get the configuration from the server. • The URL must be a non-NULL terminated ASCII string that specifies the complete path of the configuration file.

Command Default

An Easy VPN remote device cannot request a configuration from a server in a Mode Configuration Exchange.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

After the server "pushes" the URL to a Cisco Easy VPN remote device, the remote device can download the content located at the URL site and apply the configuration content to its running configuration.

Before this command can be configured, the **crypto isakmp client configuration group** command must already have been configured.

Examples

The file served by the configuration URL should have a Cisco IOS command-line interface(CLI) listing. The listing can have an optional "transient" section. The keyword to begin the transient section is "!%transient," and the keyword should be on a single line. A persistent section can be optionally identified by the keyword "!%persistent," also shown on a single line. An example of a CLI listing follows:

```
ip cef
cdp advertise-v2
!%transient
ip domain-name example.com
ntp server 10.2.3.4
```

```
ntp update-calendar
```

In the above example, the first two lines stay in the configuration even after the tunnel is disconnected (but they are not written into the nonvolatile configuration). The last three lines are effective only as long as the tunnel is "up."

The following example shows that a server has specified the URL the Easy VPN remote device must use to download the URL:

```
crypto isakmp client configuration group group1
 configuration url http://10.10.8.8/easy.cfg
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.

configuration version

To specify on a server the version that a Cisco Easy VPN remote device must use to get a particular configuration in a Mode Configuration Exchange, use the **configuration version** command in global configuration mode. To delete the version number, use the **no** form of this command.

configuration version {*version-number*}

no configuration version {*version-number*}

Syntax Description

version-number	Specifies the version of the configuration. • The version number will be an unsigned integer in the range 1 through 32767.

Command Default

A version number is not sent.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

Before this command can be configured, the **crypto isakmp client configuration group** command must already have been configured.

Examples

The following example shows that a server has specified the version number a Cisco Easy VPN remote device must use to obtain that particular configuration version:

```
crypto isakmp client configuration group group1
 configuration version 10
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.

content-length

To permit or deny HTTP traffic through the firewall on the basis of message size, use the **content-length** command in appfw-policy-http configuration mode. To remove message-size limitations from your configuration, use the **no** form of this command.

content-length {**min** *bytes* **max** *bytes* | **min** *bytes* | **max** *bytes*} **action** {**reset** | **allow**} [**alarm**]

no content-length {**min** *bytes* **max** *bytes* | **min** *bytes* | **max** *bytes*} **action** {**reset** | **allow**} [**alarm**]

Syntax Description

min *bytes*	Minimum content length, in bytes, allowed per message. Number of bytes range: 0 to 65535.
max *bytes*	Maximum content length, in bytes, allowed per message. Number of bytes range: 0 to 65535.
action	Messages whose size do not meet the minimum or exceed the maximum number of bytes are subject to the specified action (**reset** or **allow**).
reset	Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection.
allow	Forwards the packet through the firewall.
alarm	(Optional) Generates system logging (syslog) messages for the given action.

Defaults

If this command is not enabled, message size is not considered when permitting or denying HTTP messages.

Command Modes

appfw-policy-http configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

All messages exceeding the specified content-length range, will be subjected to the configured action (**reset** or **allow**).

Examples

The following example, which shows how to define the HTTP application firewall policy “mypolicy,” will not permit HTTP messages longer than 1 byte. This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule “firewall,” which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length max 1 action allow alarm
  content-type-verification match-req-resp action allow alarm
```

```
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

content-type-verification

To permit or deny HTTP traffic through the firewall on the basis of content message type, use the **content-type-verification** command in appfw-policy-http configuration mode. To disable this inspection parameter, use the **no** form of this command.

content-type-verification [**match-req-resp**] **action** {**reset** | **allow**} [**alarm**]

no content-type-verification [**match-req-resp**] **action** {**reset** | **allow**} [**alarm**]

Syntax Description

match-req-resp	(Optional) Verifies the content type of the HTTP response against the accept field of the HTTP request.
action	Messages that match the specified content type are subject to the specified action (**reset** or **allow**).
reset	Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection.
allow	Forwards the packet through the firewall.
alarm	(Optional) Generates system logging (syslog) messages for the given action.

Defaults

If this command is not issued, all traffic will be allowed.

Command Modes

appfw-policy-http configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

After the **content-type-verification** command is issued, all HTTP messages are subjected to the following inspections:

- Verify that the content type of the message header is listed as a supported content type. (See Table 20.)
- Verify that the content type of the header matches the content of the message data or entity body portion of the message.

Table 20 contains a list of supported content types.

Table 20 HTTP Header Supported Content Types

Supported Content Types
audio/*
audio/basic
audio/midi
audio/mpeg

Table 20 HTTP Header Supported Content Types (continued)

Supported Content Types
audio/x-adpcm
audio/x-aiff
audio/x-ogg
audio/x-wav
application/msword
application/octet-stream
application/pdf
application/postscript
application/vnd.ms-excel
application/vnd.ms-powerpoint
application/x-gzip
application/x-java-arching
application/x-java-xm
application/zip
image/*
image/cgf
image/gif
image/jpeg
image/png
image/tiff
image/x-3ds
image/x-bitmap
image/x-niff
image/x-portable-bitmap
image/x-portable-greymap
image/x-xpm
text/*
text/css
text/html
text/plain
text/richtext
text/sgml
text/xmcd
text/xml
video/*
video/-flc

Table 20 HTTP Header Supported Content Types (continued)

Supported Content Types
video/mpeg
video/quicktime
video/sgi
video/x-avi
video/x-fli
video/x-mng
video/x-msvideo

The following example shows how to define the HTTP application firewall policy "mypolicy." This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule "firewall," which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length max 1 action allow alarm
  content-type-verification match-req-resp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

control

To configure the control interface type and number for a redundancy group, use the **control** command in redundancy application group configuration mode**.** To remove the control interface for the redundancy group, use the **no** form of this command.

control *interface-type interface-number* **protocol** *id*

no control

Syntax Description

interface-type	Interface type.
interface-number	Interface number.
protocol	Specifies redundancy group protocol media.
id	Redundancy group protocol instance. The range is from 1 to 8.

Command Default

The control interface is not configured.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following example shows how to configure the redundancy group protocol media and instance for the control Gigabit Ethernet interface:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# control GigabitEthernet 0/0/0 protocol 1
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
data	Configures the data interface type and number for a redundancy group.
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.

Command	Description
preempt	Enables preemption on the redundancy group.
protocol	Defines a protocol instance in a redundancy group.

copy (consent-parameter-map)

To configure a consent page to be downloaded from a file server, use the **copy** command in parameter-map type consent configuration mode.

copy *src-file-name dst-file-name*

Syntax Description

src-file-name	Source file location in which the specified file will be retrieved. The source file location must be TFTP; for example, tftp://10.1.1.1/username/myfile.
dst-file-name	Destination location in which a copy of the file will be stored. The destination file should be copied to Flash; for example, flash.username.html.

Command Default

The consent page that is specified via the default parameter-map will be used.

Command Modes

Parameter-map-type consent (config-profile)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Use the **copy** command to transfer a file (consent web page) from an external server to a local file system on a device. Thus, the file name specified via the **copy** command is retrieved from the destination file location and displayed to the end user as the consent page.

When a consent webpage is displayed to an end user, the filename specified via the **file** command is used. If the file command is not configured, the destination location specified via the **copy** command is used.

Examples

In the following example, both parameter maps are to use the consent file "tftp://192.168.104.136/consent_page.html" and store it in "flash:consent_page.html":

```
parameter-map type consent consent_parameter_map
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity consent_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
parameter-map type consent default
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity test_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
```

Related Commands

Command	Description
file (consent-parameter-map)	Specifies a local filename that is to be used as the consent webpage.

copy idconf

To load a signature package in Cisco IOS Intrusion Prevention System (IPS), use the **copy idconf** command in EXEC mode.

copy *url* **idconf**

Syntax Description

url	Specifies the location from which the router loads the signature file. Available URL locations are as follows: • Local flash, such as flash:sig.xml • FTP server, such as ftp://myuser:mypass@ftp_server.sig.xml • rcp, such as rcp://myuser@rcp_server/sig.xml • TFTP server, such as tftp://tftp_server/sig.xml

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use the **copy** *url* **idconf** command to load a signature package into Cisco IOS IPS. You may wish to load a new signature package into Cisco IOS IPS if a signature (or signatures) with the current signature file is not providing your network with adequate protection from security threats. After the signature package has been loaded into the router, Cisco IOS IPS saves all signature information to the location specified via the **ip ips config location** command.

Signatures are loaded into the scanning table on the basis of importance. Parameters such as signature severity, signature fidelity rating, and time lapsed since signatures were released enable Cisco IOS IPS to compile the most important signatures first, followed by less important signatures, thereby, creating a load order and prioritizing which signatures are loaded first.

Note The **copy** *url* **idconf** command replaces the **copy ips-sdf** command.

Examples

The following example shows how to load a signature package into Cisco IOS IPS from the location "flash:IOS-S258-CLI-kd.pkg":

```
Router# copy flash:IOS-S258-CLI-kd.pkg idconf
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_BUILDS_STARTED: 17:19:47 MST Nov 14 2006
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_BUILDING: multi-string - 3 signatures - 1 of 13
engines
```

```
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_READY: multi-string - build time 4 ms - packets
for this engine will be scanned
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_BUILDING: service-http - 611 signatures - 2 of 13
engines
*Nov 14 2006 17:20:00 MST: %IPS-6-ENGINE_READY: service-http - build time 12932 ms -
packets for this engine will be scanned
*Nov 14 2006 17:20:00 MST: %IPS-6-ENGINE_BUILDING: string-tcp - 864 signatures - 3 of 13
engines
*Nov 14 2006 17:20:02 MST: %IPS-6-ENGINE_READY: string-tcp - build time 2692 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:02 MST: %IPS-6-ENGINE_BUILDING: string-udp - 74 signatures - 4 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: string-udp - build time 316 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: state - 28 signatures - 5 of 13 engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: state - build time 24 ms - packets for
this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: atomic-ip - 252 signatures - 6 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-4-META_ENGINE_UNSUPPORTED: atomic-ip 2154:0 - this
signature is a component of the unsupported META engine
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: atomic-ip - build time 232 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: string-icmp - 3 signatures - 7 of 13 e
Router# engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: string-icmp - build time 12 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-ftp - 3 signatures - 8 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-ftp - build time 8 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-rpc - 75 signatures - 9 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-rpc - build time 80 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-dns - 38 signatures - 10 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-dns - build time 20 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: normalizer - 9 signatures - 11 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: normalizer - build time 0 ms - packets for
this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-msrpc - 22 signatures - 12 of
13 engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-msrpc - build time 8 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 16344 ms
```

Related Commands

Command	Description
ip ips config-location	Specifies the location in which the router will save signature information.

copy ips-sdf

Note In Cisco IOS Release 12.4(11)T, the **copy ips-sdf** command was replaced with the **copy idconf** command. For more information, see the **copy idconf** command.

To load or save the signature definition file (SDF) in the router, use the **copy ips-sdf** command in EXEC mode.

Syntax for Loading the SDF

copy [**/erase**] *url* **ips-sdf**

Syntax for Saving the SDF

copy ips-sdf *url*

Syntax Description

/erase	(Optional) Erases the current SDF in the router before loading the new SDF. **Note** This option is typically available only on platforms with limited memory.
url	Description for the *url* argument is one of the following options: • If you want to load the SDF in the router, the *url* argument specifies the location in which to search for the SDF. • If you are saving the SDF, the *url* argument represents the location in which the SDF is saved after it has been generated. Regardless of what option the URL is used for, available URL locations are as follows: • local flash, such as flash:sig.xml • FTP server, such as ftp://myuser:mypass@ftp_server.sig.xml • rcp, such as rcp://myuser@rcp_server/sig.xml • TFTP server, such as tftp://tftp_server/sig.xml

Command Modes

EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(11)T	This command was replaced with the **copy idconf** command.

Usage Guidelines

Loading Signatures From the SDF

Issue the **copy** *url* **ips-sdf** command to load the SDF in the router from the location specified via the *url* argument. When the new SDF is loaded, it is merged with the SDF that is already loaded in the router, unless the **/erase** keyword is issued, which overwrites the current SDF with the new SDF.

Cisco IOS Intrusion Prevention System (IPS) will attempt to retrieve the SDF from each specified location in the order in which they were configured in the startup configuration. If Cisco IOS IPS cannot retrieve the signatures from any of the specified locations, the built-in signatures will be used.

If the **no ip ips sdf built-in** command is used, Cisco IOS IPS will fail to load. IPS will then rely on the configuration of the **ip ips fail** command to either fail open or fail closed.

Note For Cisco IOS Release 12.3(8)T, the SDF should be loaded directly from Flash.

After the signatures are loaded in the router, the signature engines are built. Only after the signature engines are built can Cisco IOS IPS beginning scanning traffic.

Note Whenever signatures are replaced or merged, the router is suspended while the signature engines for the newly added or merged signatures are being built. The router prompt will be available again after the engines are built.

Depending on your platform and how many signatures are being loaded, building the engine can take up to several minutes. It is recommended that you enable logging messages to monitor the engine building status.

The **ip sdf ips location** command can also be used to load the SDF. However, unlike the **copy ips-sdf** command, this command does not force and immediately load the signatures. Signatures are not loaded until the router reboots or IPS is initially applied to an interface (via the **ip ips** command).

Saving a Generated or Merges SDF

Issue the **copy ips-sdf** *url* command to save a newly created SDF file to a specified location. The next time the router is reloaded, IPS can refer to the SDF from the saved location by including the **ip ips sdf location** command in the configuration.

Tip It is recommended that you save the SDF back out to Flash. Also, you should save the file to a different name than the original attack-drop.sdf file; otherwise, you risk loosing the original file.

Examples

The following example shows how to configure the router to load and merge the attack-drop.sdf file with the default signatures. After you have merged the two files, it is recommended to copy the newly merged signatures to a separate file. The router can then be reloaded (via the **reload** command) or reinitalized to so as to recognize the newly merged file (as shown the following example)

```
!
ip ips name MYIPS
!
interface GigabitEthernet0/1
 ip address 10.1.1.16 255.255.255.0
 ip ips MYIPS in
 duplex full
 speed 100
```

```
 media-type rj45
 no negotiation auto
!
!
! Merge the flash-based SDF (attack-drop.sdf) with the built-in signatures.
copy disk2:attack-drop.sdf ips-sdf
! Save the newly merged signatures to a separate file.
copy ips-sdf disk2:my-signatures.sdf
!
! Configure the router to use the new file, my-signatures.sdf
configure terminal
ip ips sdf location disk2:my-signatures.sdf
! Reinitialize the IPS by removing the IPS rule set and reapplying the rule set.
interface gig 0/1
 no ip ips MYIPS in
!
*Apr 8 14:05:38.243:%IPS-2-DISABLED:IPS removed from all interfaces - IPS disabled
!
 ip ips MYIPS in
!
 exit
```

Related Commands

Command	Description
ip ips sdf location	Specifies the location in which the router should load the SDF.

crl

To query the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked, use the **crl** command in ca-trustpoint configuration mode. To return to the default behavior in which the router will check the URL that is embedded in the certificate, use the **no** form of this command.

crl {**query** *url* | **optional** | **best-effort**}

no crl {**query** *url* | **optional** | **best-effort**}

Syntax Description

query *url*	The Lightweight Directory Access Protocol (LDAP) URL published by the certification authority (CA) server is specified to query the CRL; for example, ldap://another_server.
optional	CRL verification is optional.
best-effort	CRL verification will be attempted, but if the CRL is unavailable, the certificate will be accepted.

Defaults

If the **query** *url* option is not enabled, the router will check the CRL distribution point (CDP) that is embedded in the certificate. The **query** *url* option does not need to be configured if the CDP that is in the certificate is formatted as a URL (for example, http:// url or ldap:// url), including the fully qualified domain name (FQDN) of the host where the CRL is held.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SX.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The query Keyword

Use the **query** *url* option if the CDP is in LDAP form, which means that the CDP location in the certificate will indicate only where the CDP is located in the directory; that is, the CDP will not indicate the actual query location for the directory.

The optional Keyword

If your router does not have the applicable CRL and is unable to obtain one, your router will reject the peer's certificate—unless you include the **optional** keyword in your configuration. If you use the **optional** keyword, your router will check the CRL if it is cached in the router memory, but it will not download the CRL from the CDP. If the **optional** keyword is configured and a CRL is not available, the certificate will always be accepted. If the **crl optional** command is configured, you cannot manually download the CRL via the **crypto ca crl request** command because the manually downloaded CRL may not be deleted after it expires. The expired CRL may cause all certificate verifications to be denied.

The best-effort Keyword

If you prefer to have the CRL checked and accept certificates if the CRL is not available, use the **best-effort** keyword. This keyword allows the router to attempt to retrieve the CRL from the CDP that is contained in the certificate (or from a different location that is specified via the **crl query** *url* command). However, if the CRL is not available, the router will accept the certificate if it is presented within its validity period and if the certificate was issued by a trusted CA.

Note The **crypto ca trustpoint** command deprecates the **crypto ca identity** and **crypto ca trusted-root** commands and all related subcommands (all ca-identity and trusted-root configuration mode commands). If you enter a ca-identity or trusted-root subcommand, the configuration mode and command will be written back as ca-trustpoint.

Examples

The following example shows how to configure your router to query the CRL with the LDAP URL that is published by the CA named "bar":

```
crypto ca trustpoint bar
 enrollment url http://bar.cisco.com
 crl query ldap://bar.cisco.com
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

crl best-effort

Note Effective with Cisco IOS Release 12.3(2)T, this command was replaced by the **revocation-check** command.

To download the certificate revocation list (CRL) but accept certificates if the CRL is not available, use the **crl best-effort** command in ca-identity configuration mode. To return to the default behavior in which CRL checking is mandatory before your router can accept a certificate, use the **no** form of this command.

Syntax Description

This command has no arguments or keywords.

Defaults

If this command is not configured, CRL checking is mandatory before your router can accept a certificate. That is, if CRL downloading is attempted and it fails, the certificate will be considered invalid and will be rejected.

Command Modes

Ca-identity configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.3(2)T	This command was replaced by the **revocation-check** command.

Usage Guidelines

When your router receives a certificate from a peer, it will search its memory for the appropriate CRL. If the appropriate CRL is in the router memory, the CRL will be used. Otherwise, the router will download the CRL from either the certificate authority (CA) or from a CRL distribution point (CDP) as designated in the certificate of the peer. Your router will then check the CRL to ensure that the certificate that the peer sent has not been revoked. (If the certificate appears on the CRL, your router will not accept the certificate and will not authenticate the peer.)

When a CA system uses multiple CRLs, the certificate of the peer will indicate which CRL applies in its CDP extension and should be downloaded by your router.

If your router does not have the applicable CRL in memory and is unable to obtain one, your router will reject the certificate of the peer—unless you include the **crl best-effort** command in your configuration. When the **crl best-effort** command is configured, your router will try to obtain a CRL, but if it cannot obtain a CRL, it will treat the certificate of the peer as not revoked.

When your router receives additional certificates from peers, the router will continue to attempt to download the appropriate CRL if it was previously unsuccessful. The **crl best-effort** command specifies only that when the router cannot obtain the CRL, the router will not be forced to reject the certificate of a peer.

Examples

The following configuration example declares a CA and permits your router to accept certificates when CRLs are not obtainable:

```
crypto ca identity myid
enrollment url http://mycaserver
crl best-effort
```

Related Commands

Command	Description
crypto ca identity	Declares the CA your router should use.

crl optional

Note Effective with Cisco IOS Release 12.3(2)T, this command was replaced by the **revocation-check** command.

To allow the certificates of other peers to be accepted without trying to obtain the appropriate CRL, use the **crl optional** command in ca-identity configuration mode. To return to the default behavior in which CRL checking is mandatory before your router can accept a certificate, use the **no** form of this command.

crl optional

no crl optional

Syntax Description

This command has no arguments or keywords.

Defaults

The router must have and check the appropriate CRL before accepting the certificate of another IP Security peer.

Command Modes

Ca-identity configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.3(2)T	This command was replaced by the **revocation-check** command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When your router receives a certificate from a peer, it will search its memory for the appropriate CRL. If the router finds the appropriate CRL, that CRL will be used. Otherwise, the router will download the CRL from either the certificate authority (CA) or from a CRL distribution point (CDP) as designated in the certificate of the peer. Your router will then check the CRL to ensure that the certificate that the peer sent has not been revoked. (If the certificate appears on the CRL, your router will not accept the certificate and will not authenticate the peer.) To instruct the router not to download the CRL and treat the certificate as not revoked, use the **crl optional** command.

Note If the CRL already exists in the memory (for example, by using the **crypto ca crl request** command to manually download the CRL), the CRL will still be checked even if the **crl optional** command is configured.

Examples

The following example declares a CA and permits your router to accept certificates without trying to obtain a CRL. This example also specifies a nonstandard retry period and retry count.

```
crypto ca identity myca
 enrollment url http://ca_server
 enrollment retry-period 20
 enrollment retry-count 100
 crl optional
```

Related Commands

Command	Description
crypto ca identity	Declares the CA your router should use.

crl query

If you have to query the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked and you have to provide the Lightweight Directory Access Protocol (LDAP) server information, use the **crl query** command in ca-trustpoint configuration mode. To return to the default behavior, assuming that the CRL distribution point (CDP) has a complete LDAP URL, use **no** form of this command.

crl query ldap://*hostname***:**[*port*]

no crl query ldap://*hostname***:**[*port*]

Syntax Description

ldap://*hostname*	Query is made to the hostname of the LDAP server that serves the CRL for the certification authority (CA) server (for example, ldap://myldap.cisco.com).
:*port*	(Optional) Port number of the LDAP server (for example, ldap://myldap.cisco.com:3899).

Defaults

Not enabled. If **crl query ldap://***hostname***:**[*port*] is not enabled, the router assumes that the CDP that is embedded in the certificate is a complete URL (for example, ldap:myldap.cisco.com/CN=myCA,O=Cisco) and uses it to download the CRL.

If the port number is not configured, the default LDAP server port 389 will be used.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(8)T	This command replaced the **query url** command.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When Cisco IOS software tries to verify a peer certificate (for example, during Internet Key Exchange [IKE] or Secure Sockets Layer [SSL] handshake), it queries the CRL to ensure that the certificate has not been revoked. To locate the CRL, it first looks for the CDP extension in the certificate. If the extension exists, it is used to download the CRL. Otherwise, the Simple Certificate Enrollment Protocol (SCEP) GetCRL mechanism is used to query the CRL from the CA server directly (some CA servers do not support this method).

Cisco IOS software supports three types of CDP:

- HTTP URL (Example1: http://10.10.10.10:81/myca.crl)
- LDAP URL (Example 2: ldap://10.10.10.10:3899/CN=myca, O=cisco or Example 3: ldap:///CN=myca, O=cisco)
- LDAP/X.500 DN (Example 4: CN=myca, O=cisco)

To locate the CRL, a complete URL needs to be formed. As a result, Example 3 and Example 4 still require the hostname and the port number. The **ldap://***hostname***:**[*port*} keywords and arguments are used to provide this information.

Note The **crypto ca trustpoint** command replaces the **crypto ca identity** and **crypto ca trusted-root** commands and all related subcommands (all ca-identity and trusted-root configuration mode commands). If you enter a ca-identity or trusted-root subcommand, the configuration mode and command will be written back as ca-trustpoint.

Examples

The following example shows how to configure your router to query the CRL with the LDAP URL that is published by the CA named "bar":

```
crypto ca trustpoint mytp
 enrollment url http://bar.cisco.com
 crl query ldap://bar.cisco.com:3899
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
revocation-check	Checks the revocation status of a certificate.

crl-cache delete-after

To configure the maximum time a router will cache a certificate revocation list (CRL), use the **crl-cache delete-after** command in ca-trustpoint configuration mode. To enable default CRL caching, use the **no** form of this command.

crl-cache delete-after *time*

no crl-cache delete-after *time*

Syntax Description

time	The maximum lifetime of a CRL in minutes.

Command Default

A CRL is deleted from the cache when the CRL default lifetime expires.

Command Modes

Ca-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
12.4(9)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

Use this command to limit the amount of time a router will cache a CRL. You may use the **crl-cache delete-after** command to force a router to download a CRL before the existing CRL expires by configuring a value shorter than the default lifetime of the CRL.

By default, a new CRL will be downloaded after the currently cached CRL expires. The **crl-cache delete-after** command does not effect any currently cached CRLs. The configured lifetime will only effect CRLs downloaded after this command is configured.

When the maximum CRL time expires, the cached CRL will be deleted from the router cache. A new copy of the CRL will be downloaded from the issuing certificate authority (CA) the next time the router has to validate a certificate.

Note Only the **crl-cache none** command or the **crl-cache delete-after** command may be specified. If both commands are entered for a trustpoint, the last command executed will take effect and a message will be displayed to the user.

Examples

The following example shows how to configure a maximum lifetime of 2 minutes for all CRLs associated with the CA1 trustpoint:

```
crypto pki trustpoint CA1
 enrollment url http://CA1:80
 ip-address FastEthernet0/0
 crl query ldap://ldap_CA1
```

```
 revocation-check crl
 crl-cache delete-after 2
```

The current CRL is still cached immediately after executing the example configuration shown above:

```
Router# show crypto pki crls

CRL Issuer Name:
    cn=name Cert Manager,ou=pki,o=company.com,c=US
    LastUpdate: 18:57:42 GMT Nov 26 2005
    NextUpdate: 22:57:42 GMT Nov 26 2005
    Retrieved from CRL Distribution Point:
      ldap://ldap.company.com/CN=name Cert Manager,O=company.com
```

When the current CRL expires, a new CRL is then downloaded to the router at the NextUpdate time and the **crl-cache delete-after** command takes effect. This newly cached CRL and all subsequent CRLs will be deleted after a maximum lifetime of 2 minutes.

You can verify that the CRL will be cached for 2 minutes by executing the **show crypto pki crls** command. Note that the NextUpdate time is 2 minutes after the LastUpdate time.

```
Router# show crypto pki crls

CRL Issuer Name:
    cn=name Cert Manager,ou=pki,o=company.com,c=US
    LastUpdate: 22:57:42 GMT Nov 26 2005
    NextUpdate: 22:59:42 GMT Nov 26 2005
    Retrieved from CRL Distribution Point:
      ldap://ldap.company.com/CN=name Cert Manager,O=company.com
```

Related Commands

Command	Description
crl-cache none	Disables CRL caching.

crl-cache none

To disable certificate revocation list (CRL) caching, use the **crl-cache none** command in ca-trustpoint configuration mode. To enable default CRL caching, use the **no** form of this command.

crl-cache none

no crl-cache none

Syntax Description

This command has no arguments or keywords.

Command Default

CRL caching is enabled.

Command Modes

Ca-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
12.4(9)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

Use this command to disable CRL caching for all CRLs associated with a trustpoint. By default, a new CRL is issued when the currently cached CRL expires.

The **crl-cache none** command does not effect any currently cached CRLs. All CRLs downloaded after this command is configured will not be cached.

This functionality is useful is when a certification authority (CA) issues CRLs with no expiration date or with expiration dates far into the future–days or weeks.

Note Only the **crl-cache none** command or the **crl-cache delete-after** command may be specified. If both commands are entered for a trustpoint, the last command executed will take effect and a message will be displayed.

Examples

The following example shows how to disable CRL caching for all CRLs associated with the CA1 trustpoint:

```
crypto pki trustpoint CA1
 enrollment url http://CA1:80
 ip-address FastEthernet0/0
 crl query ldap://ldap_CA1
 revocation-check crl
 crl-cache none
```

The current CRL is still cached immediately after executing the example configuration shown above:

```
Router# show crypto pki crls

CRL Issuer Name:
    cn=name Cert Manager,ou=pki,o=company.com,c=US
    LastUpdate: 18:57:42 GMT Nov 26 2005
    NextUpdate: 22:57:42 GMT Nov 26 2005
    Retrieved from CRL Distribution Point:
      ldap://ldap.company.com/CN=name Cert Manager,O=company.com
```

When the current CRL expires, a new CRL is then downloaded to the router at the NextUpdate time. The **crl-cache none** command takes effect and all CRLs for the trustpoint are no longer cached; caching is disabled. You can verify that no CRL is cached by executing the **show crypto pki crls** command. No output will be shown because there are no CRLs cached.

Related Commands

Command	Description
crl-cache delete-after	Configures the maximum lifetime of a CRL.

crypto aaa attribute list

To define an authentication, authorization, and accounting (AAA) attribute list of per-user attributes on a local Easy VPN server, use the **crypto aaa attribute list** command in crypto isakmp group configuration mode. To remove the AAA attribute list, use the **no** form of this command.

crypto aaa attribute list *list-name*

no crypto aaa attribute list *list-name*

Syntax Description

list-name	Name of the local attribute list.

Command Default

A local attribute list is not defined.

Command Modes

Crypto isakmp group configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

There is no limit to the number of lists that can be defined (except for NVRAM storage limits).

Examples

The following example shows that per-user attributes have been defined on a local Easy VPN AAA server:

```
!

aaa new-model
!
!
aaa authentication login default local
aaa authentication login noAAA none
aaa authorization network default local
!
aaa attribute list per-group
 attribute type inacl "per-group-acl" service ike protocol ip mandatory
!
aaa session-id common
!
resource policy
!
ip subnet-zero
!
!
ip cef
!
!
username example password 0 example
!
```

```
!
crypto isakmp policy 3
 authentication pre-share
 group 2
crypto isakmp xauth timeout 90
!
crypto isakmp client configuration group PerUserAAA
 key cisco
 pool dpool
 crypto aaa attribute list per-group
!
crypto isakmp profile vi
 match identity group PerUserAAA
 isakmp authorization list default
 client configuration address respond
 client configuration group PerUserAAA
 virtual-template 1
!
!
crypto ipsec transform-set set esp-3des esp-sha-hmac
!
crypto ipsec profile vi
 set transform-set set
 set isakmp-profile vi
!
!
interface GigabitEthernet0/0
 description 'EzVPN Peer'
 ip address 192.168.1.1 255.255.255.128
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto

interface Virtual-Template1 type tunnel
 ip unnumbered GigabitEthernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vi
!
ip local pool dpool 10.5.0.1 10.5.0.10
ip classless
!
no ip http server
no ip http secure-server
!
!
ip access-list extended per-group-acl
 permit tcp any any
 deny   icmp any any
logging alarm informational
logging trap debugging
!
control-plane
!
gatekeeper
 shutdown
```

```
!
line con 0
line aux 0
 stopbits 1
line vty 0 4
!
!
end
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.

crypto ca authenticate

Note This command was replaced by the **crypto pki authenticate** command effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXE.

To authenticate the certification authority (by getting the certificate of the CA), use the **crypto ca authenticate** command in global configuration mode.

crypto ca authenticate *name*

Syntax Description

name	Specifies the name of the CA. This is the same name used when the CA was declared with the **crypto ca identity** command.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command is required when you initially configure CA support at your router.

This command authenticates the CA to your router by obtaining the self-signed certificate of the CA that contains the public key of the CA. Because the CA signs its own certificate, you should manually authenticate the public key of the CA by contacting the CA administrator when you perform this command.

If you are using RA mode (using the **enrollment mode ra** command) when you issue the **crypto ca authenticate** command, then registration authority signing and encryption certificates will be returned from the CA as well as the CA certificate.

This command is not saved to the router configuration. However. the public keys embedded in the received CA (and RA) certificates are saved to the configuration as part of the RSA public key record (called the "RSA public key chain").

Note If the CA does not respond by a timeout period after this command is issued, the terminal control will be returned so it will not be tied up. If this happens, you must re-enter the command. Cisco IOS software will not recognize CA certificate expiration dates set for beyond the year 2049. If the validity period of the CA certificate is set to expire after the year 2049, the following error message will be displayed when authentication with the CA server is attempted:

```
error retrieving certificate :incomplete chain
```

If you receive an error message similar to this one, check the expiration date of your CA certificate. If the expiration date of your CA certificate is set after the year 2049, you must reduce the expiration date by a year or more.

Examples

In the following example, the router requests the certificate of the CA. The CA sends its certificate and the router prompts the administrator to verify the certificate of the CA by checking the CA certificate's fingerprint. The CA administrator can also view the CA certificate's fingerprint, so you should compare what the CA administrator sees to what the router displays on the screen. If the fingerprint on the router's screen matches the fingerprint viewed by the CA administrator, you should accept the certificate as valid.

```
Router(config)# crypto ca authenticate myca
Certificate has the following attributes:
Fingerprint: 0123 4567 89AB CDEF 0123
Do you accept this certificate? [yes/no] y#
```

Related Commands

Command	Description
debug crypto pki transactions	Displays debug messages for the trace of interaction (message type) between the CA and the router.
show crypto pki certificates	Displays information about your certificate, the certificate of the CA, and any RA certificates.

crypto ca cert validate

Note This command was replaced by the **crypto pki cert validate** command effective with Cisco IOS Release 12.3(8)T and 12.2(18)SXE.

To determine if a trustpoint has been successfully authenticated, a certificate has been requested and granted, and if the certificate is currently valid, use the **crypto ca cert validate** command in global configuration mode.

crypto ca cert validate *trustpoint*

Syntax Description

trustpoint	The trustpoint to be validated.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The **crypto ca cert validate** command validates the router's own certificate for a given trustpoint. Use this command as a sanity check after enrollment to verify that the trustpoint is properly authenticated, a certificate has been requested and granted for the trustpoint, and that the certificate is currently valid. A certificate is valid if it is signed by the trustpoint certification authority (CA), not expired, and so on.

Examples

The following examples show the possible output from the **crypto ca cert validate** command:

```
Router(config)# crypto ca cert validate ka

Validation Failed: trustpoint not found for ka


Router(config)# crypto ca cert validate ka

Validation Failed: can't get local certificate chain


Router(config)# crypto ca cert validate ka

Certificate chain has 2 certificates.
Certificate chain for ka is valid


Router(config)# crypto ca cert validate ka
```

```
Certificate chain has 2 certificates.
Validation Error: no certs on chain


Router(config)# crypto ca cert validate ka

Certificate chain has 2 certificates.
Validation Error: unspecified error
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the certification authority that the router should use.
show crypto pki trustpoints	Displays the trustpoints that are configured in the router.

crypto ca certificate chain

Note This command was replaced by the **crypto pki certificate chain** command effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXE.

To enter the certificate chain configuration mode, use the **crypto ca certificate chain** command in global configuration mode. (You need to be in certificate chain configuration mode to delete certificates.)

crypto ca certificate chain *name*

Syntax Description

name	Specifies the name of the CA. Use the same name as when you declared the CA using the **crypto pki trustpoint** command.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command puts you into certificate chain configuration mode. When you are in certificate chain configuration mode, you can delete certificates using the **certificate** command.

Examples

The following example deletes the router's certificate. In this example, the router had a general-purpose RSA key pair with one corresponding certificate. The show command is used to determine the serial number of the certificate to be deleted.

```
Router# show crypto ca certificates

Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: 0123456789ABCDEF0123456789ABCDEF
  Key Usage: General Purpose

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set

Router# configure terminal
Rrouter(config)# crypto ca certificate chain myca
Router(config-cert-chain)# no certificate 0123456789ABCDEF0123456789ABCDEF
```

```
% Are you sure you want to remove the certificate [yes/no]? yes
% Be sure to ask the CA administrator to revoke this certificate.
Router(config-cert-chain)# exit
```

Related Commands

Command	Description
certificate	Adds certificates manually.

crypto ca certificate map

Note This command was replaced by the **crypto pki certificate map** command effective with Cisco IOS Release 12.3(7)T, 12.2(18)SXD, and 12.2(18)SXE.

To define certificate-based access control lists (ACLs), use the **crypto ca certificate map** command in ca-certificate-map configuration mode. To remove the certificate-based ACLs, use the **no** form of this command.

crypto ca certificate map *label sequence-number*

no crypto ca certificate map *label sequence-number*

Syntax Description

label	A user-specified label that is referenced within the **crypto ca trustpoint** command.
sequence-number	A number that orders the ACLs with the same label. ACLs with the same label are processed from lowest to highest sequence number. When an ACL is matched, processing stops with a successful result.

Defaults

No default behavior or value.

Command Modes

Ca-certificate-map configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Issuing this command places the router in CA certificate map configuration mode where you can specify several certificate fields together with their matching criteria. The general form of these fields is as follows:

```
field-name match-criteria match-value
```

The *field-name* in the above example is one of the certificate fields. Field names are similar to the names used in the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) X.509 standard. The **name** field is a special field that matches any subject name or related name field in the certificate, such as the **alt-subject-name**, **subject-name**, and **unstructured-subject-name** fields.

- **alt-subject-name**—Case-insensitive string.
- **expires-on**—Date field in the format dd mm yyyy hh:mm:ss or mmm dd yyyy hh:mm:ss.
- **issuer-name**—Case-insensitive string.
- **name**—Case-insensitive string.
- **subject-name**—Case-insensitive string.

- **unstructured-subject-name**—Case-insensitive string.
- **valid-start**—Date field in the format dd mm yyyy hh:mm:ss or mmm dd yyyy hh:mm:ss.

Note The time portion is optional in both the **expires-on** date and **valid-start** field and defaults to 00:00:00 if not specified. The time is interpreted according to the time zone offset configured for the router. The string **utc** can be appended to the date and time when they are configured as Universal Time, Coordinated (UTC) rather than local time.

The *match-criteria* in the example is one of the following logical operators:

- **eq**—equal (valid for name and date fields)
- **ne**—not equal (valid for name and date fields)
- **co**—contains (valid only for name fields)
- **nc**—does not contain (valid only for name fields)
- **lt**—less than (valid only for date fields)
- **ge**—greater than or equal to (valid only for date fields)

The *match-value* is a case-insensitive string or a date.

Examples

The following example shows how to configure a certificate-based ACL that will allow any certificate issued by Cisco Systems to an entity within the cisco.com domain. The label is Cisco, and the sequence is 10.

```
crypto ca certificate map Cisco 10
 issuer-name co Cisco Systems
 unstructured-subject-name co cisco.com
```

The following example accepts any certificate issued by Cisco Systems for an entity with DIAL or organizationUnit component ou=WAN. This certificate-based ACL consists of two separate ACLs tied together with the common label Group. Because the check for DIAL has a lower sequence number, it is performed first. Note that the string “DIAL” can occur anywhere in the subjectName field of the certificate, but the string WAN must be in the organizationUnit component.

```
crypto ca certificate map Group 10
 issuer-name co Cisco Systems
 subject-name co DIAL
crypto ca certificate map Group 20
 issuer-name co Cisco Systems
 subject-name co ou=WAN
```

Case is ignored in string comparisons; therefore, DIAL in the previous example will match dial, DIAL, Dial, and so on. Also note that the component identifiers (o=, ou=, cn=, and so on) are not required unless it is desirable that the string to be matched occurs in a specific component of the name. (Refer to the ITU-T security standards for more information about certificate fields and components such as ou=.)

If a component identifier is specified in the match string, the exact string, including the component identifier, must appear in the certificate. This requirement can present a problem if more than one component identifier is included in the match string. For example, “ou=WAN,o=Cisco Systems” will not match a certificate with the string “ou=WAN,ou=Engineering,o=Cisco Systems” because the “ou=Engineering” string separates the two desired component identifiers.

To match both “ou=WAN” and “o=Cisco Systems” in a certificate while ignoring other component identifiers, you could use this certificate map:

```
crypto ca certificate map Group 10
 subject-name co ou=WAN
 subject-name co o=Cisco
```

Any space character proceeding or following the equal sign (=) character in component identifiers is ignored. Therefore “o=Cisco” in the proceeding example will match “o = Cisco,” “o= Cisco,” “o =Cisco,” and so on.

Related Commands

Command	Description
crypto pki trustpoint	Declares the CA that your router should use.

crypto ca certificate query (ca-trustpoint)

Note This command was replaced by the **crypto pki certificate query** (**ca-trustpoint**) command effective with Cisco IOS Release 12.3(7)T, 12.2(18)SXD, and 12.2(18)SXE.

To specify that certificates should not be stored locally but retrieved from a certification authority (CA) trustpoint, use the **crypto ca certificate query** command in ca-trustpoint configuration mode. To cause certificates to be stored locally per trustpoint, use the **no** form of this command.

crypto ca certificate query

no crypto ca certificate query

Syntax Description

This command has no arguments or keywords.

Defaults

CA trustpoints are stored locally in the router's NVRAM.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Normally, certain certificates are stored locally in the router's NVRAM, and each certificate uses a moderate amount of memory. To save NVRAM space, you can use this command to put the router into query mode, preventing certificates from being stored locally; instead, they are retrieved from a specified CA trustpoint when needed. This will save NVRAM space but could result in a slight performance impact.

The **crypto ca certificate query** command is a subcommand for each trustpoint; thus, this command can be disabled on a per-trustpoint basis.

Before you can configure this command, you must enable the **crypto pki trustpoint** command, which puts you in ca-trustpoint configuration mode.

Note This command replaces the **crypto ca certificate query** command in global configuration mode. Although you can still enter the global configuration command, the configuration mode and command will be written back as ca-trustpoint.

Examples

The following example shows how to prevent certificates and certificate revocation lists (CRLs) from being stored locally on the router; instead, they are retrieved from the "ka" trustpoint when needed.

```
crypto ca trustpoint ka
```

```
.
.
.
crypto ca certificate query
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the CA that your router should use.

crypto ca certificate query (global)

The **crypto ca certificate query** command in global configuration mode is replaced by the **crypto ca certificate query** command in ca-trustpoint configuration mode. See the **crypto ca certificate query** command for more information.

crypto ca crl request

Note Effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXE, this command was replaced by the **crypto pki crl request** command.

To request that a new certificate revocation list (CRL) be obtained immediately from the certification authority, use the **crypto ca crl request** command in global configuration mode.

crypto ca crl request *name*

Syntax Description

name	Specifies the name of the CA. This is the same name used when the CA was declared with the **crypto pki trustpoint** command.

Defaults

Normally, the router requests a new CRL when it is verifying a certificate and there is no CRL cached.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.3(7)T	This command was replaced by the **crypto pki crl request** command.

Usage Guidelines

A CRL lists all the certificates of the network device that have been revoked. Revoked certificates will not be honored by your router; therefore, any IPSec device with a revoked certificate cannot exchange IP Security traffic with your router.

The first time your router receives a certificate from a peer, it will download a CRL from the CA. Your router then checks the CRL to make sure the certificate of the peer has not been revoked. (If the certificate appears on the CRL, it will not accept the certificate and will not authenticate the peer.)

A CRL can be reused with subsequent certificates until the CRL expires. If your router receives the certificate of a peer after the applicable CRL has expired, it will download the new CRL.

If your router has a CRL which has not yet expired, but you suspect that the contents of the CRL are out of date, use the **crypto ca crl request** command to request that the latest CRL be immediately downloaded to replace the old CRL.

This command is not saved to the configuration.

Note This command should be used only after the trustpoint is enrolled.

Examples

The following example immediately downloads the latest CRL to your router:

```
crypto ca crl request
```

crypto ca enroll

Note This command was replaced by the **crypto pki enroll** command effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXE.

To obtain the certificate(s) of your router from the certification authority, use the **crypto ca enroll** command in global configuration mode. To delete a current enrollment request, use the **no** form of this command.

crypto ca enroll *name*

no crypto ca enroll *name*

Syntax Description

name	Specifies the name of the CA. Use the same name as when you declared the CA using the **crypto pki trustpoint** command.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command requests certificates from the CA for all of your router's RSA key pairs. This task is also known as enrolling with the CA. (Technically, enrolling and obtaining certificates are two separate events, but they both occur when this command is issued.)

Your router needs a signed certificate from the CA for each RSA key pairs of your router; if you previously generated general purpose keys, this command will obtain the one certificate corresponding to the one general purpose RSA key pair. If you previously generated special usage keys, this command will obtain two certificates corresponding to each of the special usage RSA key pairs.

If you already have a certificate for your keys you will be unable to complete this command; instead, you will be prompted to remove the existing certificate first. (You can remove existing certificates with the **no certificate** command.)

The **crypto ca enroll** command is not saved in the router configuration.

Note If your router reboots after you issue the **crypto ca enroll** command but before you receive the certificate(s), you must reissue the command.

Responding to Prompts

When you issue the **crypto ca enroll** command, you are prompted a number of times.

First, you are prompted to create a challenge password. This password can be up to 80 characters in length. This password is necessary in the event that you ever need to revoke your router's certificate(s). When you ask the CA administrator to revoke your certificate, you must supply this challenge password as a protection against fraudulent or mistaken revocation requests.

Note This password is not stored anywhere, so you need to remember this password.

If you lose the password, the CA administrator may still be able to revoke the router's certificate but will require further manual authentication of the router administrator identity.

You are also prompted to indicate whether or not your router's serial number should be included in the obtained certificate. The serial number is not used by IP Security or Internet Key Exchange but may be used by the CA to either authenticate certificates or to later associate a certificate with a particular router. (Note that the serial number stored is the serial number of the internal board, not the one on the enclosure.) Ask your CA administrator if serial numbers should be included. If you are in doubt, include the serial number.

Normally, you would not include the IP address because the IP address binds the certificate more tightly to a specific entity. Also, if the router is moved, you would need to issue a new certificate. Finally, a router has multiple IP addresses, any of which might be used with IPSec.

If you indicate that the IP address should be included, you will then be prompted to specify the interface of the IP address. This interface should correspond to the interface that you apply your crypto map set to. If you apply crypto map sets to more than one interface, specify the interface that you name in the **crypto map local-address** command.

Examples

In the following example, a router with a general-purpose RSA key pair requests a certificate from the CA. When the router displays the certificate fingerprint, the administrator verifies this number by calling the CA administrator, who checks the number. The fingerprint is correct, so the router administrator accepts the certificate.

There can be a delay between when the router administrator sends the request and when the certificate is actually received by the router. The amount of delay depends on the CA method of operation.

```
Router(config)# crypto ca enroll myca
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password: <mypassword>
Re-enter password: <mypassword>

% The subject name in the certificate will be: myrouter.example.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: 03433678
% Include an IP address in the subject name [yes/no]? yes
Interface: ethernet0/0
Request certificate from CA [yes/no]? yes
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificates' command will also show the fingerprint.
```

Some time later, the router receives the certificate from the CA and displays the following confirmation message:

```
Router(config)#   Fingerprint: 01234567 89ABCDEF FEDCBA98 75543210

%CRYPTO-6-CERTRET: Certificate received from Certificate Authority

Router(config)#
```

If necessary, the router administrator can verify the displayed Fingerprint with the CA administrator.

If there is a problem with the certificate request and the certificate is not granted, the following message is displayed on the console instead:

```
%CRYPTO-6-CERTREJ: Certificate enrollment request was rejected by Certificate Authority
```

The subject name in the certificate is automatically assigned to be the same as the RSA key pair's name. In the above example, the RSA key pair was named "myrouter.example.com." (The router assigned this name.)

Requesting certificates for a router with special usage keys would be the same as the previous example, except that two certificates would have been returned by the CA. When the router received the two certificates, the router would have displayed the same confirmation message:

```
%CRYPTO-6-CERTRET: Certificate received from Certificate Authority
```

Related Commands

Command	Description
debug crypto pki messages	Displays debug messages for the details of the interaction (message dump) between the CA and the router.
debug crypto pki transactions	Displays debug messages for the trace of interaction (message type) between the CA and the router.
show crypto pki certificates	Displays information about your certificate, the certificate of the CA, and any RA certificates.

crypto ca export pem

Note This command was replaced by the **crypto pki export pem** command effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXE.

To export certificates and Rivest, Shamir, and Adelman (RSA) keys that are associated with a trustpoint in a privacy-enhanced mail (PEM)-formatted file, use the **crypto ca export pem** command in global configuration mode.

crypto ca export *trustpoint* **pem** {**terminal** | **url** *url*} {**3des** | **des**} *passphrase*

Syntax Description

trustpoint	Name of the trustpoint that the associated certificate and RSA key pair will export. The *trustpoint* argument must match the name that was specified via the **crypto pki trustpoint** command.
terminal	Certificate and RSA key pair that will be displayed in PEM format on the console terminal.
url *url*	URL of the file system where your router should export the certificate and RSA key pairs.
3des	Export the trustpoint using the Triple Data Encryption Standard (3DES) encryption algorithm.
des	Export the trustpoint using the DES encryption algorithm.
passphrase	Passphrase that is used to encrypt the PEM file for import. **Note** The passphrase can be any phrase that is at least eight characters in length; it can include spaces and punctuation, excluding the question mark (?), which has special meaning to the Cisco IOS parser.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The **crypto ca export pem** command allows you to export certificate and RSA key pairs in PEM-formatted files. The PEM files can then be imported back into the Cisco IOS router (via the **crypto pki import pem** command) or other public key infrastructure (PKI) applications.

Examples

The following example shows how to generate and export the RSA key pair "aaa" and certificates of the router in PEM files that are associated with the trustpoint "mycs":

```
Router(config)# crypto key generate rsa general-keys label aaa exportable
The name for the keys will be:aaa
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes.
!
How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]
!
Router(config)# crypto pki trustpoint mycs
Router(ca-trustpoint)# enrollment url http://mycs
Router(ca-trustpoint)# rsakeypair aaa
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate mycs
Certificate has the following attributes:
Fingerprint:C21514AC 12815946 09F635ED FBB6CF31
% Do you accept this certificate? [yes/no]:y
Trustpoint CA certificate accepted.
!
Router(config)# crypto pki enroll mycs
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this password to the CA
Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.

Password:
Re-enter password:

% The fully-qualified domain name in the certificate will be:Router
% The subject name in the certificate will be:bizarro.cisco.com
% Include the router serial number in the subject name? [yes/no]:n
% Include an IP address in the subject name? [no]:n
Request certificate from CA? [yes/no]:y
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

Router(config)# Fingerprint: 8DA777BC 08477073 A5BE2403 812DD157

00:29:11:%CRYPTO-6-CERTRET:Certificate received from Certificate Authority

Router(config)# crypto ca export aaa pem terminal 3des cisco123

% CA certificate:
-----BEGIN CERTIFICATE-----
MIICAzCCAa2gAwIBAgIBATANBgkqhkiG9w0BAQUFADBOMQswCQYDVQQGEwJVUzES
<snip>
waDeNOSI3WlDa0AWq5DkVBkxwgn0TqIJXJOCttjHnWHK1LMcMVGn
-----END CERTIFICATE-----

% Key name:aaa
    Usage:General Purpose Key
-----BEGIN RSA PRIVATE KEY-----
Proc-Type:4,ENCRYPTED
DEK-Info:DES-EDE3-CBC,ED6B210B626BC81A

Urguv0jnjwOgowWVUQ2XR5nbzzYHI2vGLunpH/IxIsJuNjRVjbAAUpGk7VnPCT87
<snip>
kLCOtxzEv7JHc72gMku9uUlrLSnFH5slzAtoC0czfU4=
```

```
-----END RSA PRIVATE KEY-----

% Certificate:
-----BEGIN CERTIFICATE-----
MIICTjCCAfigAwIBAgICIQUwDQYJKoZIhvcNAQEFBQAwTjELMAkGA1UEBhMCVVMx
<snip>
6xlBaIsuMxnHmr89KkKkYlU6
-----END CERTIFICATE-----
```

Related Commands

Command	Description
crypto pki import pem	Imports certificates and RSA keys to a trustpoint from PEM-formatted files.
crypto pki trustpoint	Declares the CA that your router should use.
enrollment	Specifies the enrollment parameters of a CA.

crypto ca export pkcs12

Note This command was replaced by the **crypto pki export pkcs12** command effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXE.

To export Rivest, Shamir, and Adelman (RSA) keys within a PKCS12 file at a specified location, use the **crypto ca export pkcs12** command in global configuration mode.

crypto ca export *trustpointname* **pkcs12** *destination url passphrase*

Syntax Description

trustpointname	Name of the trustpoint who issues the certificate that a user is going to export. When you export the PKCS12 file, the trustpoint name is the RSA key name.
destination url	Location of the PKCS12 file to which a user wants to import the RSA key pair.
passphrase	Passphrase that is used to encrypt the PKCS12 file for export.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

The **crypto ca export pkcs12** command creates a PKCS 12 file that contains an RSA key pair. The PKCS12 file, along with a certificate authority (CA), is exported to the location that you specify with the destination URL. If you decide not to import the file to another router, you must delete the file.

Security Measures

Keep the PKCS12 file stored in a secure place with restricted access.

An RSA keypair is more secure than a passphrase because the private key in the key pair is not known by multiple parties. When you export an RSA key pair to a PKCS#12 file, the RSA key pair now is only as secure as the passphrase.

To create a good passphrase, be sure to include numbers, as well as both lowercase and uppercase letters. Avoid publicizing the passphrase by mentioning it in e-mail or cell phone communications because the information could be accessed by an unauthorized user.

Examples

The following example exports an RSA key pair with a trustpoint name “mytp” to a Flash file:

```
Router(config)# crypto ca export mytp pkcs12 flash:myexport mycompany
```

Related Commands

Command	Description
crypto pki import pkcs12	Imports RSA keys.

crypto ca identity

The **crypto ca identity** command is replaced by the **crypto ca trustpoint** command. See the **crypto ca trustpoint** command for more information.

crypto ca import

Note This command was replaced by the **crypto pki import** command effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXD.

To import a certificate manually via TFTP or as a cut-and-paste at the terminal, use the **crypto ca import** command in global configuration mode.

crypto ca import *name* **certificate**

Syntax Description

name **certificate**	Name of the certification authority (CA). This name is the same name used when the CA was declared with the **crypto pki trustpoint** command.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

You must enter the **crypto ca import** command twice if usage keys (signature and encryption keys) are used. The first time the command is entered, one of the certificates is pasted into the router; the second time the command is entered, the other certificate is pasted into the router. (It does not matter which certificate is pasted first.)

Examples

The following example shows how to import a certificate via cut-and-paste. In this example, the CA trustpoint is "MS."

```
crypto pki trustpoint MS
 enroll terminal
 crypto pki authenticate MS
!
crypto pki enroll MS
crypto ca import MS certificate
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the CA that your router should use.
enrollment	Specifies the enrollment parameters of your CA.
enrollment terminal	Specifies manual cut-and-paste certificate enrollment.

crypto ca import pem

Note This command was replaced by the **crypto pki import pem** command effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXE.

To import certificates and Rivest, Shamir, and Adelman (RSA) keys to a trustpoint from privacy-enhanced mail (PEM)-formatted files, use the **crypto ca import pem** command in global configuration mode.

crypto ca import *trustpoint* **pem** [**usage-keys**] {**terminal** | **url** *url*} [**exportable**] *passphrase*

Syntax Description

trustpoint	Name of the trustpoint that is associated with the imported certificates and RSA key pairs. The *trustpoint* argument must match the name that was specified via the **crypto pki trustpoint** command.
usage-keys	(Optional) Specifies that two RSA special usage key pairs will be imported (that is, one encryption pair and one signature pair), instead of one general-purpose key pair.
terminal	Certificates and RSA key pairs will be manually imported from the console terminal.
url *url*	URL of the file system where your router should import the certificates and RSA key pairs.
exportable	(Optional) Specifies that the imported RSA key pair can be exported again to another Cisco device such as a router.
passphrase	Passphrase that is used to encrypt the PEM file for import. **Note** The passphrase can be any phrase that is at least eight characters in length; it can include spaces and punctuation, excluding the question mark (?), which has special meaning to the Cisco IOS parser.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The **crypto ca import pem** command allows you import certificates and RSA key pairs in PEM-formatted files. The files can be previously exported from another router or generated from other public key infrastructure (PKI) applications.

Examples

The following example shows how to import PEM files to trustpoint "ggg" via TFTP:

```
Router(config)# crypto ca import ggg pem url tftp://10.1.1.2/johndoe/msca cisco1234

% Importing CA certificate...
Address or name of remote host [10.1.1.2]?
Destination filename [johndoe/msca.ca]?
Reading file from tftp://10.1.1.2/johndoe/msca.ca
Loading johndoe/msca.ca from 10.1.1.2 (via Ethernet0):!
[OK - 1082 bytes]

% Importing private key PEM file...
Address or name of remote host [10.1.1.2]?
Destination filename [johndoe/msca.prv]?
Reading file from tftp://10.1.1.2/johndoe/msca.prv
Loading johndoe/msca.prv from 10.1.1.2 (via Ethernet0):!
[OK - 573 bytes]

% Importing  certificate PEM file...
Address or name of remote host [10.1.1.2]?
Destination filename [johndoe/msca.crt]?
Reading file from tftp://10.1.1.2/johndoe/msca.crt
Loading johndoe/msca.crt from 10.1.1.2 (via Ethernet0):!
[OK - 1289 bytes]
% PEM files import succeeded.
Router(config)#
```

Related Commands

Command	Description
crypto pki export pem	Exports certificates and RSA keys that are associated with a trustpoint in a PEM-formatted file.
crypto pki trustpoint	Declares the CA that your router should use.
enrollment	Specifies the enrollment parameters of a CA.

crypto ca import pkcs12

Note This command was replaced by the **crypto pki import pkcs12** command effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXE.

To import Rivest, Shamir, and Adelman (RSA) keys, use the **crypto ca import pkcs12** command in global configuration mode.

crypto ca import *trustpointname* **pkcs12** *source url passphrase*

Syntax Description

trustpointname	Name of the trustpoint who issues the certificate that a user is going to export or import. When importing, the trustpoint name will become the RSA key name.
source url	The location of the PKCS12 file to which a user wants to export the RSA key pair.
passphrase	Passphrase that must be entered to undo encryption when the RSA keys are imported.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

When you enter the **cyrpto ca import pkcs12** command, a ke pair and a trustpoint are generated. If you then decide you want to remove the key pair and trustpoint that were generated, enter the **crypto key zeroize rsa** command to zeroize the key pair and enter the **no crypto ca trustpoint** command to remove the trustpoint.

Note After you import RSA keys to a target router, you cannot export those keys from the target router to another router.

Examples

In the following example, an RSA key pair that has been associated with the trustpoint "forward" is to be imported:

```
Router(config)# crypto ca import forward pkcs12 flash:myexport mycompany
```

Related Commands

Command	Description
crypto pki export pkcs12	Exports RSA keys.
crypto pki trustpoint	Declares the CA that your router should use.
crypto key zeroize rsa	Deletes all RSA keys from your router.

crypto ca profile enrollment

Note This command was replaced with the **crypto pki profile enrollment** command effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXE.

To define an enrollment profile, use the **crypto ca profile enrollment** command in global configuration mode. To delete all information associated with this enrollment profile, use the **no** form of this command.

crypto ca profile enrollment *label*

no crypto ca profile enrollment *label*

Syntax Description

label	Name for the enrollment profile; the enrollment profile name must match the name specified in the **enrollment profile** command.

Defaults

An enrollment profile does not exist.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

Before entering this command, you must specify a named enrollment profile using the **enrollment profile** in ca-trustpoint configuration mode.

After entering the **crypto ca profile enrollment** command, you can use any of the following commands to define the profile parameters:

- **authentication command**—Specifies the HTTP command that is sent to the certification authority (CA) for authentication.
- **authentication terminal**—Specifies manual cut-and-paste certificate authentication requests.
- **authentication url**—Specifies the URL of the CA server to which to send authentication requests.
- **enrollment command**—Specifies the HTTP command that is sent to the CA for enrollment.
- **enrollment terminal**—Specifies manual cut-and-paste certificate enrollment.
- **enrollment url**—Specifies the URL of the CA server to which to send enrollment requests.
- **parameter**—Specifies parameters for an enrollment profile. This command can be used only if the **authentication command** or the **enrollment command** is used.

Note The **authentication url**, **enrollment url**, **authentication terminal**, and **enrollment terminal** commands allow you to specify different methods for certificate authentication and enrollment, such as TFTP authentication and manual enrollment.

Examples

The following example shows how to define the enrollment profile named "E" and associated profile parameters:

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial

crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
enrollment profile	Specifies that an enrollment profile can be used for certificate authentication and enrollment.

crypto ca trusted-root

The **crypto ca trusted-root** command is replaced by the **crypto ca trustpoint** command. See the **crypto ca trustpoint** command for more information.

crypto ca trustpoint

Note Effective with Cisco IOS Release 12.3(8)T, 12.2(18)SXD, and 12.2(18)SXE, the **crypto ca trustpoint** command is replaced with the **crypto pki trustpoint** command. See the **crypto pki trustpoint** command for more information.

To declare the certification authority (CA) that your router should use, use the **crypto ca trustpoint** command in global configuration mode. To delete all identity information and certificates associated with the CA, use the **no** form of this command.

crypto ca trustpoint *name*

no crypto ca trustpoint *name*

Syntax Description

name	Creates a name for the CA. (If you previously declared the CA and just want to update its characteristics, specify the name you previously created.)

Defaults

Your router does not recognize any CAs until you declare a CA using this command.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(15)T	The **match certificate** subcommand was introduced.
12.3(7)T	This command was replaced by the **crypto pki trustpoint** command. You can still enter the **crypto ca trusted-root** or **crypto ca trustpoint** command, but the command will be written in the configuration as "crypto pki trustpoint."

Usage Guidelines

Use the **crypto ca trustpoint** command to declare a CA, which can be a self-signed root CA or a subordinate CA. Issuing the **crypto ca trustpoint** command puts you in ca-trustpoint configuration mode.

You can specify characteristics for the trustpoint CA using the following subcommands:

- **crl**—Queries the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked.
- **default (ca-trustpoint)**—Resets the value of ca-trustpoint configuration mode subcommands to their defaults.
- **enrollment**—Specifies enrollment parameters (optional).
- **enrollment http-proxy**—Accesses the CA by HTTP through the proxy server.

- **match certificate**—Associates a certificate-based access control list (ACL) defined with the **crypto ca certificate map** command.
- **primary**—Assigns a specified trustpoint as the primary trustpoint of the router.
- **root**—Defines the Trivial File Transfer Protocol (TFTP) to get the CA certificate and specifies both a name for the server and a name for the file that will store the CA certificate.

Note Beginning with Cisco IOS Release 12.2(8)T, the **crypto ca trustpoint** command unified the functionality of the **crypto ca identity** and **crypto ca trusted-root** commands, thereby replacing these commands. Although you can still enter the **crypto ca identity** and **crypto ca trusted-root** commands, the configuration mode and command will be written in the configuration as "crypto ca trustpoint."

Examples

The following example shows how to declare the CA named "ka" and specify enrollment and CRL parameters:

```
crypto ca trustpoint ka
 enrollment url http://kahului:80
```

The following example shows a certificate-based access control list (ACL) with the label "Group" defined in a **crypto ca certificate map** command and included in the **match certificate** subcommand of the **crypto ca | pki trustpoint** command:

```
crypto ca certificate map Group 10
 subject-name co ou=WAN
 subject-name co o=Cisco
!
crypto ca trustpoint pki
 match certificate Group
```

Related Commands

Command	Description
crl	Queries the CRL to ensure that the certificate of the peer has not been revoked.
default (ca-trustpoint)	Resets the value of a ca-trustpoint configuration subcommand to its default.
enrollment	Specifies the enrollment parameters of your CA.
enrollment http-proxy	Accesses the CA by HTTP through the proxy server.
primary	Assigns a specified trustpoint as the primary trustpoint of the router.
root	Obtains the CA certificate via TFTP.

crypto call admission limit

To specify the maximum number of Internet Key Exchange (IKE) and IPsec security associations (SAs) that the router can establish before IKE begins rejecting new SA requests, use the **crypto call admission limit** command in global configuration mode. To disable this feature, use the **no** form of this command.

crypto call admission limit {**all in-negotiation-sa** *number* | **ipsec sa** *number* | **ike** {**in-negotiation-sa** *number* | **sa** *number*}}

no crypto call admission limit {**all in-negotiation-sa** *number* | **ipsec sa** *number* | **ike** {**in-negotiation-sa** *number* | **sa** *number*}}

Syntax Description

all	Indicates the total number of sessions in negotiation.
in-negotiation-sa	Specifies the maximum number of in-negotiation IKE SAs allowed.
number	Value for SAs. The range is from 0 to 99999.
ipsec	Configures the crypto Call Admission Control (CAC) active IPsec SA limit.
sa	Specifies the number of active IKE and IPsec SAs allowed.
ike	Configures the crypto CAC active IKE SA limit.

Command Default

No maximum number of IKE and IPsec SAs is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1 on the Cisco 6500 and Cisco 7600 series routers.
12.4(6)T	This command was modified. The **in-negotiation-sa** keyword and *number* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA on the Cisco 7600 series routers. The **in-negotiation-sa** keyword and *number* argument were not added to this release.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH. The **in-negotiation-sa** keyword and *number* argument were not added to this release.
15.1(3)T	This command was modified. The **all** and **ipsec** keywords were added.

Usage Guidelines

Use this command to limit the number of IKE SAs permitted to or from a router. By limiting the number of dynamic tunnels that can be created to the router, you can prevent the router from being overwhelmed if it is suddenly inundated with IKE SA requests. The ideal limit depends on the particular platform, the network topology, the application, and traffic patterns. When the specified limit is reached, IKE rejects

all new SA requests. If you specify an IKE SA limit that is less than the current number of active IKE SAs, a warning is displayed, but SAs are not terminated. New SA requests are rejected until the active SA count is below the configured limit.

The **ipsec sa** *number* and **ike sa** *number* keyword and argument pairs in the **crypto call admission limit** command set the limit for the number of established IPsec SAs and IKE SAs.

The **all in-negotiation-sa** *number* and **ike in-negotiation-sa** *number* keyword and argument pairs in the **crypto call admission limit** command limit all the SAs in negotiation and IKE SAs in negotiation.

Examples

The following example shows how to specify a maximum limit of 50 IKE SAs before IKE begins rejecting new SA requests:

```
Router(config)# crypto call admission limit ike sa 50
```

The following example shows how to specify a maximum limit of 100 in-negotiation IKE SAs before IKE begins rejecting new SA requests:

```
Router(config)# crypto call admission limit ike in-negotiation-sa 100
```

Related Commands

Command	Description
show crypto call admission statistics	Monitors Crypto CAC statistics.

crypto connect vlan

To create an interface VLAN for an IPSec VPN SPA and enter crypto-connect mode, use the **crypto connect vlan** command in interface configuration mode. To remove the interface VLAN status from the VLAN, use the **no** form of this command.

crypto connect vlan *vlan-id*

no crypto connect [**vlan** *vlan-id*]

Syntax Description

vlan-id	VLAN ID number.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can enter the **crypto connect vlan** command only from the following:

- The associated port VLAN interface when the EtherChannel interface (port-channel interface) and participating interfaces are switch ports.
- The EtherChannel interface when the EtherChannel interface (port-channel interface) and participant interfaces are routed ports.

The **crypto engine subslot** command is only available for VLANs prior to the VLANs being made interface VLANs by the **crypto connect vlan** command.

When you enter the **crypto connect vlan** command, a target VLAN is made an interface VLAN if and only if the target VLAN is not currently an interface VLAN, and the target VLAN has been added to an inside trunk port using the **crypto engine subslot** command. If the VLAN has been added to more than one inside trunk port, the **crypto connect vlan** command is rejected.

The **no crypto engine subslot** command is allowed only after you enter the **no crypto connect vlan** command, or before you enter the **crypto connect vlan** command.

When you remove an interface VLAN from an inside trunk port and a corresponding crypto engine subslot configuration state exists, then that crypto engine subslot configuration state is not removed. If you remove a VLAN that has a crypto engine subslot configuration state, you need to manually add it back to recover. While in this inconsistent state, any attempt to enter the **no crypto connect vlan** command is rejected.

When you enter the **no crypto connect vlan** command, the interface VLAN status is removed from a VLAN. Any associated crypto engine subslot configuration state is not altered.

Examples

The following example adds port 2/1 to the outside access port VLAN and connects the outside access port VLAN to the inside interface VLAN:

```
Router(config)# interface Vlan101
Router(config-if)# ip address 192.168.101.1 255.255.255.0
Router(config-if)# crypto map cmap
Router(config-if)# crypto engine subslot 3/0

Router(config-if)# interface GigabitEthernet2/1
Router(config-if)# crypto connect vlan 101
```

Related Commands

Command	Description
crypto engine subslot	Assign an interface VLAN that requires encryption to the IPSec VPN SPA.
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.
show crypto vlan	Displays the VPN running state for an IPSec VPN SPA.

crypto ctcp

To configure Cisco Tunneling Control Protocol (cTCP) encapsulation for Easy VPN, use the **crypto ctcp** command in global configuration mode. To remove the cTCP encapsulation, use the **no** form of this command.

crypto ctcp [**keepalive** *number-of-seconds* | **port** *port-number*]

no crypto ctcp [**keepalive** *number-of-seconds* | **port** *port-number*]

Syntax Description

keepalive	(Optional) Sets the interval of cTCP keepalives that are sent by the remote device. **Note** This command is configured on the remote device.
number-of-seconds	(Optional) Number of seconds between the keepalives. Value = 5 through 3600. If the **keepalive** keyword is not configured, the default is 5.
port	(Optional) Port number that cTCP will listen to. Up to 10 numbers can be configured. **Note** This keyword is configured only on the server.
port-number	(Optional) Actual port number. Value = 1 through 65535. If the **port** keyword is not configured, the default port number is 10000.

Command Default

cTCP encapsulation is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(9)T	The **crypto ctcp** command was introduced.
12.4(20)T	The **keepalive** keyword and *number-of-seconds* argument were added.

Usage Guidelines

If cTCP is enabled on a port, any application that uses that port will not function.

When cTCP encapsulation is enabled on the router, only packets less than or equal to 1407 in size can pass through the IPsec tunnel with the Don't Fragment (DF) bit set. If an attempt is made to send a larger size packet, the following syslog message is generated:

```
CRYPTO_ENGINE: locally-sourced pkt w/DF bit set is too big,ip->tl=1450, mtu=1407
```

Note If a Cisco IOS device is acting as a remote device, it has to send keepalives periodically to keep Network Address Translation (NAT) or firewall sessions from timing out.

Examples

The following example shows that cTCP encapsulation has been configured on port 120:

```
Router (config)# crypto ctcp port 120
```

The following example shows that the cTCP keepalive interval has been set at 30 seconds:

```
Router (config)# crypto ctcp keepalive 30
```

Related Commands

Command	Description
clear crypto ctcp	Clears cTCP encapsulation.
ctcp port	Sets the port number for cTCP encapsulation for Easy VPN.
debug crypto ctcp	Displays information about a cTCP session.
show crypto ctcp	Displays information about a cTCP session.

crypto dynamic-map

To create a dynamic crypto map entry and enter crypto map configuration command mode, use the **crypto dynamic-map** command in global configuration mode. To delete a dynamic crypto map set or entry, use the **no** form of this command.

crypto dynamic-map *dynamic-map-name dynamic-seq-num*

no crypto dynamic-map *dynamic-map-name* [*dynamic-seq-num*]

Syntax Description

dynamic-map-name	Specifies the name of the dynamic crypto map set.
dynamic-seq-num	Specifies the number of the dynamic crypto map entry.

Defaults

No dynamic crypto maps exist.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(15)T	This command was modified. All changes to PFS settings in the dynamic crypto map template are immediately passed on to the instantiated crypto map PFS settings.

Usage Guidelines

Use dynamic crypto maps to create policy templates that can be used when processing negotiation requests for new security associations from a remote IP security peer, even if you do not know all of the crypto map parameters required to communicate with the remote peer (such as the peer's IP address). For example, if you do not know about all the IPsec remote peers in your network, a dynamic crypto map allows you to accept requests for new security associations from previously unknown peers. (However, these requests are not processed until the Internet Key Exchange authentication has completed successfully.)

When a router receives a negotiation request via IKE from another IPsec peer, the request is examined to see if it matches a crypto map entry. If the negotiation does not match any explicit crypto map entry, it will be rejected unless the crypto map set includes a reference to a dynamic crypto map.

The dynamic crypto map is a policy template; it will accept "wildcard" parameters for any parameters not explicitly stated in the dynamic crypto map entry. This allows you to set up IPsec security associations with a previously unknown IPsec peer. (The peer still must specify matching values for the nonwildcard IPsec security association negotiation parameters.))

If the router accepts the peer's request, at the point that it installs the new IPsec security associations it also installs a temporary crypto map entry. This entry is filled in with the results of the negotiation. At this point, the router performs normal processing, using this temporary crypto map entry as a normal entry, even requesting new security associations if the current ones are expiring (based upon the policy specified in the temporary crypto map entry). Once the flow expires (that is, all of the corresponding security associations expire), the temporary crypto map entry is removed.

If changes are made to the Perfect Forward Secrecy (PFS) settings in the dynamic crypto map template,the changes are passed on to the PFS settings in the instantiated crypto map. During the next rekey process the new settings are used to negotiate with the remote peer.

Dynamic crypto map sets are not used for initiating IPsec security associations. However, they are used for determining whether or not traffic should be protected.

The only configuration required in a dynamic crypto map is the **set transform-set** command. All other configuration is optional.

Dynamic crypto map entries, like regular static crypto map entries, are grouped into sets. After you define a dynamic crypto map set (which commonly contains only one map entry) using this command, you include the dynamic crypto map set in an entry of the "parent" crypto map set using the **crypto map** (IPsec global configuration) command. The parent crypto map set is then applied to an interface.

You should make crypto map entries referencing dynamic maps the lowest priority map entries, so that negotiations for security associations will try to match the static crypto map entries first. Only after the negotiation request does not match any of the static map entries do you want it to be evaluated against the dynamic map.

To make a dynamic crypto map the lowest priority map entry, give the map entry referencing the dynamic crypto map the highest *seq-num* of all the map entries in a crypto map set.

For both static and dynamic crypto maps, if unprotected inbound traffic matches a **permit** statement in an access list, and the corresponding crypto map entry is tagged as "IPsec," then the traffic is dropped because it is not IPsec protected. (This is because the security policy as specified by the crypto map entry states that this traffic must be IPsec protected.)

For static crypto map entries, if outbound traffic matches a **permit** statement in an access list and the corresponding security association (SA) is not yet established, the router will initiate new SAs with the remote peer. In the case of dynamic crypto map entries, if no SA existed, the traffic would simply be dropped (because dynamic crypto maps are not used for initiating new SAs).

Note Use care when using the **any** keyword in **permit** entries in dynamic crypto maps. If it is possible for the traffic covered by such a **permit** entry to include multicast or broadcast traffic, the access list should include **deny** entries for the appropriate address range. Access lists should also include **deny** entries for network and subnet broadcast traffic, and for any other traffic that should not be IPsec protected.

Examples

The following example shows how to configure an IPsec crypto map set.

Crypto map entry "mymap 30" references the dynamic crypto map set "mydynamicmap," which can be used to process inbound security association negotiation requests that do not match "mymap" entries 10 or 20. In this case, if the peer specifies a transform set that matches one of the transform sets specified in "mydynamicmap," for a flow "permitted" by the access list 103, IPsec will accept the request and set up security associations with the remote peer without previously knowing about the remote peer. If accepted, the resulting security associations (and temporary crypto map entry) are established according to the settings specified by the remote peer.

The access list associated with "mydynamicmap 10" is also used as a filter. Inbound packets that match a **permit** statement in this list are dropped for not being IPsec protected. (The same is true for access lists associated with static crypto maps entries.) Outbound packets that match a **permit** statement without an existing corresponding IPsec SA are also dropped.

```
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
 set peer 10.0.0.2
crypto map mymap 20 ipsec-isakmp
 match address 102
 set transform-set my_t_set1 my_t_set2
 set peer 10.0.0.3
crypto map mymap 30 ipsec-isakmp dynamic mydynamicmap
!
crypto dynamic-map mydynamicmap 10
 match address 103
 set transform-set my_t_set1 my_t_set2 my_t_set3
```

Related Commands

Command	Description
crypto map (global IPsec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map (interface IPsec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPsec traffic.
match address (IPsec)	Specifies an extended access list for a crypto map entry.
set peer (IPsec)	Specifies an IPsec peer in a crypto map entry.
set pfs	Specifies that IPsec should ask for PFS when requesting new security associations for this crypto map entry, or that IPsec requires PFS when receiving requests for new security associations.
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPsec security associations.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto engine accelerator logs	Displays a dynamic crypto map set.
show crypto map (IPsec)	Displays the crypto map configuration.

crypto-engine

To enter the QoS policy map configuration mode for the IPsec VPN module, use the **crypto-engine** command in interface configuration mode.

crypto-engine

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	Support for this command was introduced.

Usage Guidelines

Once you enter the **crypto-engine** command, the prompt changes to the following:

```
Router(config-crypto-engine)#
```

The following crypto engine configuration commands are available when you enter the **crypto-engine** command:

- **default**—Sets a command to its defaults.
- **exit**—Exit service-flow submode.
- **no**—Negates a command or set its defaults.
- **service-policy output** *policy-map-name*—Configures the service policy by assigning a policy map to the output of an interface.

Examples

The following example shows how to apply the policy map to tunnel egress traffic:

```
Router(config)# interface tunnel1
Router(config-if)# crypto-engine
Router(config-crypto-engine)# service-policy output crypto1
```

Related Commands

Command	Description
show policy-map interface	Displays the statistics and configurations of the QoS policies attached to the tunnel interface.

crypto engine accelerator

Note Effective with Cisco IOS Release 12.3(11)T, this command is replaced by the **crypto engine aim**, **crypto engine em**, **crypto engine nm**, **crypto engine onboard**, and **crypto engine slot** commands. See these commands for more information.

To enable the onboard hardware accelerator of the router for IP security (IPsec) encryption, use the **crypto engine accelerator** command in global configuration mode. To disable the use of the onboard hardware IPsec accelerator, and thereby perform IPsec encryption or decryption in software, use the **no** form of this command.

crypto engine accelerator

no crypto engine accelerator

Syntax Description

This command has no arguments or keywords.

Defaults

The hardware accelerator for IPsec encryption is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced for the Cisco 1700 series router and other Cisco routers that support hardware accelerators for IPsec encryption.
12.1(3)XL	Support was added for the Cisco uBR905 cable access router.
12.2(2)XA	Support was added for the Cisco uBR925 cable access router.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented for the AIM-VPN/EPII and AIM-VPN/HPII on the following platforms: Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.
12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.3(4)T	The AIM-VPN/BPII was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.3(11)T	This command was replaced by the **crypto engine aim**, **crypto engine em**, **crypto engine nm**, **crypto engine onboard**, and **crypto engine slot** commands.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is not normally needed for typical operations because the onboard hardware accelerator of the router is enabled for IPsec encryption by default. The hardware accelerator should not be disabled except on instruction from Cisco Technical Assistance Center (TAC) personnel.

Examples

The following example shows how to disable the onboard hardware accelerator of the router for IPsec encryption. This disabling is normally needed only after the accelerator has been disabled for testing or debugging purposes.

```
Router(config)# no crypto engine accelerator

Warning! all current connections will be torn down.
Do you want to continue? [yes/no]:
```

Related Commands

Command	Description
clear crypto engine accelerator counter	Resets the statistical and error counters for the hardware accelerator to zero.
crypto ca	Defines the parameters for the certification authority used for a session.
crypto cisco	Defines the encryption algorithms and other parameters for a session.
crypto dynamic-map	Creates a dynamic map crypto configuration for a session.
crypto ipsec	Defines the IPSec security associations and transformation sets.
crypto isakmp	Enables and defines the IKE protocol and its parameters.
crypto key	Generates and exchanges keys for a cryptographic session.
crypto map	Creates and modifies a crypto map for a session.
debug crypto engine accelerator control	Displays each control command as it is given to the crypto engine.
debug crypto engine accelerator packet	Displays information about each packet sent for encryption and decryption.
show crypto engine accelerator ring	Displays the contents of command and transmits rings for the crypto engine.
show crypto engine accelerator sa-database	Displays the active (in-use) entries in the crypto engine SA database.
show crypto engine accelerator statistic	Displays the current run-time statistics and error counters for the crypto engine.
show crypto engine brief	Displays a summary of the configuration information for the crypto engine.
show crypto engine configuration	Displays the version and configuration information for the crypto engine.
show crypto engine connections	Displays a list of the current connections maintained by the crypto engine.

crypto engine aim

To reenable an advanced integration module (AIM), use the **crypto engine aim** command in global configuration mode. To disable an AIM encryption module, use the **no** form of this command.

crypto engine aim *aim-slot-number*

no crypto engine aim *aim-slot-number*

Syntax Description

aim-slot-number	Slot number to which an AIM is to be reenabled or disabled.

Defaults

An AIM is neither reenabled nor disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)T	This command was introduced. This command replaces the **crypto engine accelerator** command.

Usage Guidelines

The **crypto engine accelerator** command will still be usable for a while, but if it is used, only the **crypto engine aim** command will be saved to the running and startup (nonvolatile memory) configuration.

Examples

The following example shows that the AIM in slot 0 is to be reenabled:

```
crypto engine aim 0
```

The following example shows that the AIM in slot 0 is to be disabled:

```
no crypto engine aim 0
```

crypto engine em

To enable the hardware accelerator of an expansion slot for IP security (IPsec) encryption, use the **crypto engine em** command in global configuration mode. To disable the hardware accelerator of the expansion slot, use the **no** form of this command.

crypto engine em *slot-number*

no crypto engine em *slot-number*

Syntax Description

slot-number	Slot number to which the hardware accelerator of the expansion slot is to be enabled or disabled (applies to slots 0 through 3).

Defaults

The hardware accelerator is neither enabled nor disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)T	This command was introduced. This command replaces the **crypto engine accelerator** command.

Usage Guidelines

The **crypto engine accelerator** command will still be usable for a while, but if it is used, only the **crypto engine em** command will saved to the running and startup (nonvolatile memory) configuration.

Examples

The following example shows that the hardware accelerator of expansion slot 1 is to be enabled:

```
crypto engine em 1
```

The following example shows that the hardware accelerator of expansion slot 1 is to be disabled:

```
no crypto engine em 1
```

crypto engine mode vrf

To enable VRF-Aware mode for the IPSec VPN SPA, use the **crypto engine mode vrf** command in global configuration mode. To disable VRF-aware mode, use the **no** form of this command.

crypto engine mode vrf

no crypto engine mode vrf

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The VRF-Aware IPSec feature introduces IPSec tunnel mapping to Multiprotocol Label Switching (MPLS) VPNs.

Using the VRF-Aware IPSec feature, you can map IPSec tunnels to VPN routing and forwarding instances (VRFs) using a single public-facing address.

Unlike other IPSec VPN SPA feature configurations, when configuring VRF-Aware features, you do not use the **crypto connect vlan** command.

Examples

The following example shows a VRF-Aware IPSec implementation:

```
ip vrf pepsi
 rd 1000:1
 route-target export 1000:1
 route-target import 1000:1
!
ip vrf coke
 rd 2000:1
 route-target export 2000:1
 route-target import 2000:1

crypto engine mode vrf

interface vlan 100
 ip vrf forwarding pepsi
 ip address 10.2.1.1 255.255.255.0
 crypto engine subslot 3/0
 crypto map map100

interface vlan 200
 ip vrf forwarding coke
 ip address 10.2.1.1 255.255.255.0
 crypto engine subslot 3/0
```

```
 crypto map map200

interface gi1/1 (hidden VLAN 1000)
 ip address 171.1.1.1
 crypto engine subslot 3/0

! BASIC MPLS CONFIGURATION
mpls label protocol ldp
tag-switching tdp router-id Loopback0
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
!
! CONFIGURE THE INTERFACE CONNECTED TO THE MPLS BACKBONE WITH LABEL/TAG SWITCHING
interface GigabitEthernet2/12
 ip address 20.1.0.34 255.255.255.252
 logging event link-status
 speed nonegotiate
 mpls label protocol ldp
tag-switching ip
```

Related Commands

Command	Description
crypto engine subslot	Assigns an interface VLAN that requires encryption to the IPSec VPN SPA.
ip vrf	Configures a VRF routing table and enters VRF configuration mode.
ip vrf forwarding	Associates a VRF with an interface or subinterface.
vrf	Defines the VRF to which the IPSec tunnel will be mapped.

crypto engine nm

To enable the onboard hardware accelerator of a network module for IP security (IPsec) encryption, use the **crypto engine nm** command in global configuration mode. To disable the accelerator of the network module, use the **no** form of this command.

crypto engine nm *slot-number*

no crypto engine nm *slot-number*

Syntax Description

slot-number	Slot number to which the hardware accelerator of a network module is to be enabled or disabled (applies to slots 0 through 5).

Defaults

The hardware accelerator is neither enabled nor disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)T	This command was introduced. This command replaces the **crypto engine accelerator** command.

Usage Guidelines

The **crypto engine accelerator** command will still be usable for a while, but if it is used, only the **crypto engine nm** command will saved to the running and startup (nonvolatile memory) configuration.

Examples

The following example shows that the hardware accelerator of the network module in slot 0 is to be enabled:

```
crypto engine nm 0
```

The following example shows that the hardware accelerator of the network module in slot 0 is to be disabled:

```
no crypto engine nm 0
```

crypto engine onboard

To enable the hardware accelerator of an onboard module for IP security (IPsec) encryption, use the **crypto engine onboard** command in global configuration mode. To disable the hardware accelerator of the onboard module, use the **no** form of this command.

crypto engine onboard *slot-number*

no crypto engine onboard *slot-number*

Syntax Description

slot-number	Slot number to which the hardware accelerator of the onboard module is to be enabled or disabled (applies to slots 0 and 1).

Defaults

The hardware accelerator is neither enabled nor disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)T	This command was introduced. This command replaces the **crypto engine accelerator** command.

Usage Guidelines

The **crypto engine accelerator** command will still be usable for a while, but if it is used, only the **crypto engine onboard** command will saved to the running and startup (nonvolatile memory) configuration.

Examples

The following example shows that the hardware accelerator of the onboard module in slot 1 is to be enabled:

```
crypto engine onboard 1
```

The following example shows that the hardware accelerator of the onboard module in slot 1 is to be disabled:

```
no crypto engine onboard 1
```

crypto engine slot

To reenable the onboard hardware accelerator in a service adapter, use the **crypto engine slot** command in global configuration mode. To disable the hardware accelerator in the service adapter, use the **no** form of this command.

crypto engine slot *slot-number*

no crypto engine slot *slot-number*

Syntax Description

slot-number	Slot number to which the hardware accelerator in a service adapter is to be reenabled or disabled (applies to slots 1 through 6).

Defaults

The hardware accelerator is neither enabled nor disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)T	This command was introduced. This command replaces the **crypto engine accelerator** command.

Usage Guidelines

The **crypto engine accelerator** command will still be usable for a while, but if it is used, only the **crypto engine slot** command will saved to the running and startup (nonvolatile memory) configuration.

Examples

The following example shows that the hardware accelerator of the service adaptor in slot 2is to be enabled:

```
crypto engine slot 2
```

The following example shows that the hardware accelerator of the service adaptor in slot 2 is to be disabled:

```
no crypto engine slot 2
```

crypto engine slot (interface)

To assign an interface VLAN, Virtual Routing and Forwarding (VRF) tunnel interface, or Front-door VRF (FVRF) interface that requires encryption to the IPSec VPN Shared Port Adapter (SPA), use the **crypto engine slot** command in interface configuration mode. The command usage and syntax varies based on whether you are in crypto-connect mode or VRF mode. In crypto-connect mode, the command is applied to interface VLANs and only the *slot*/*subslot* arguments are specified; in VRF-mode, the command is applied to interface VLANs, tunnel interfaces, or FVRF interfaces and either the **inside** or **outside** keyword must also be specified. To remove the interface, use the corresponding **no** form of this command.

Crypto-Connect Mode Syntax

crypto engine slot *slot*

no crypto engine slot *slot*

VRF Mode Syntax

crypto engine slot *slot* {**inside** | **outside**}

no crypto engine slot *slot* {**inside** | **outside**}

Syntax Description

slot	Chassis slot number where the Cisco 7600 SSC-400 card is located. Refer to the appropriate hardware manual for slot information. For SIPs and SSCs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide.
inside	(VRF Mode Only) Identifies the interface as an interface VLAN or tunnel interface.
outside	(VRF Mode Only) Identifies the interface as an FVRF interface.

Command Default

No interface is assigned.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRA	This command was introduced into Cisco IOS Release 12.2(33)SRA to support the IPSec VPN SPA on Cisco 7600 series routers and Catalyst 6500 series switches.
12.2(33)SRE	This command was modified. The *subslot* argument was removed.

Usage Guidelines

Usage guidelines vary based on whether you are in crypto-connect mode or VRF mode:

Crypto-Connect Mode Usage Guidelines

With this command, you do not need to explicitly add interface VLANs to the IPSec VPN SPA inside trunk port.

It is strongly recommended that you use the **crypto engine slot** command instead of manually adding and removing VLANs from the inside trunk port.

When you add an interface VLAN to an inside trunk port and that interface VLAN is not already added to another inside trunk port, the crypto engine slot configuration state on the interface VLAN is combined. If the interface VLAN is already added to another inside trunk port, the command is rejected.

You should not try to add all VLANs at one time (If you attempt this, you can recover by manually removing the VLANs from the inside trunk port.)

In crypto-connect mode, the **crypto engine slot** command is used in conjunction with the **crypto connect vlan** command.

In crypto-connect mode, the **crypto engine slot** command is only available for VLANs prior to the VLANs being made interface VLANs by the **crypto connect vlan** command.

The **crypto engine slot** command is rejected if you enter it on a crypto-connected interface VLAN whose current crypto engine slot configuration is different from the subslot specified in the **crypto engine slot** command. To change the crypto engine slot configuration on an interface VLAN, you must ensure that the VLAN is not crypto-connected.

If you change the crypto engine slot configuration on an interface VLAN, any IPSec and IKE SAs that are currently active on that interface VLAN are deleted.

If you enter the **no crypto engine slot** command and the interface VLAN is crypto-connected, the **no crypto engine slot** command is rejected. The **no crypto engine slot** command is allowed only after you enter the **no crypto connect vlan** command, or before you enter the **crypto connect vlan** command.

When you remove an interface VLAN from an inside trunk port and a corresponding crypto engine slot configuration state exists, then that crypto engine slot configuration state is not removed. If you remove a VLAN that has a crypto engine slot configuration state, you need to manually add it back to recover. While in this inconsistent state, any attempt to enter the **no crypto connect vlan** command is rejected.

When you enter the **no crypto connect vlan** command, the interface VLAN status is removed from a VLAN. Any associated crypto engine slot configuration state is not altered.

When you write the configuration or show the configuration, the crypto engine slot configuration state is expressed in the context of the associated interface VLAN. The interface VLAN is also shown as having been added to the appropriate inside trunk port. This is the case even if the configuration was loaded from a legacy (pre-crypto engine slot) configuration file, or if VLANs were manually added instead of being added through the **crypto engine slot** command.

By editing the **crypto engine slot** commands and inside trunk port VLANs, it is possible to produce an inconsistent configuration file.

VRF Mode Usage Guidelines

When configuring an interface VLAN or tunnel interface in VRF mode, the **crypto-engine slot inside** command must be specified.

When configuring an FVRF interface in VRF mode, the **crypto-engine slot outside** command must be specified.

In VRF mode, the **crypto-connect vlan** command is not used.

In Cisco IOS Release 12.2(33)SRE and later releases the *subslot* argument was removed.

Examples

The following crypto-connect mode example shows how to assign VLAN interface 101 to the IPSec VPN SPA in slot 3, subslot 0:

```
Router(config)# interface Vlan101
Router(config-if)# ip address 192.168.101.1 255.255.255.0
Router(config-if)# crypto map cmap
Router(config-if)# crypto engine slot 3/0

Router(config)# interface GigabitEthernet2/1
Router(config-if)# crypto connect Vlan101
```

The following VRF mode example shows how to assign VLAN interface 101 to the IPSec VPN SPA in slot 3, subslot 0:

```
Router(config)# interface Vlan101
Router(config-if)# ip vrf forwarding abc
Router(config-if)# ip address 10.2.1.1 255.255.255.0
Router(config-if)# crypto engine slot 3/0 inside
Router(config-if)# crypto map map100
```

The following VRF mode example shows how to assign Tunnel interface 1 to the IPSec VPN SPA in slot 4, subslot 0:

```
Router(config)# interface Tunnel1
Router(config)# ip vrf forwarding abc
Router(config-if)# ip address 10.1.1.254 255.255.255.0
Router(config-if)# tunnel source 172.1.1.1
Router(config-if)# tunnel destination 100.1.1.1
Router(config-if)# tunnel mode ipsec profile tp
Router(config-if)# crypto engine slot 4/0 inside
```

The following VRF mode example assigns the WAN-side interface GigabitEthernet1/1 to the IPSec VPN SPA in slot 3, subslot 0:

```
Router(config)# interface GigabitEthernet1/1
Router(config-if)# ip address 171.1.1.1 255.255.255.0
Router(config-if)# crypto engine slot 3/0 outside
```

Related Commands

Command	Description
crypto connect vlan	Creates an interface VLAN for an IPSec VPN SPA and enters crypto-connect mode.
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.
ip vrf forwarding	Associates a VRF with an interface.
show crypto vlan	Displays the VPN running state for an IPSec VPN SPA.
tunnel vrf	Associates a VRF instance with a specific tunnel interface.

crypto gdoi gm

For group members to change the IP security (IPsec) security association (SA) status, use the **crypto gdoi gm** command in privileged EXEC mode.

crypto gdoi gm group *group-name* {**ipsec direction inbound optional** | **ipsec direction inbound only** | **ipsec direction both**}

Syntax Description

group *group-name*	Name of the group.
ipsec direction inbound optional	Allows a group member to change the IPsec SA status to inbound optional. IPsec SA will accept cipher or plain text or both and will encrypt the packet before forwarding it.
ipsec direction inbound only	Allows a group member to change the IPsec SA status to inbound only. IPsec SA will accept cipher or plain text or both and will forward the packet in clear text.
ipsec direction both	Allows a group member to change the IPsec SA status to both inbound and outbound. IPsec SA will accept only cipher text and will encrypt the packet before forwarding it.

Command Default

If the **sa receive-only** command is specified on the key server, the group member remains in receive-only mode.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

This command is executed on group members. This command and its various keywords aid in testing individual group members and verifies that the group members are encrypting or decrypting traffic. This command and its keywords can be used only after the **sa receive-only** command has been configured on the key server.

The **ipsec direction inbound optional** keyword is used for situations in which all group members have been instructed to install the IPsec SAs as inbound only but for which a group member wants to install the IPsec SAs as inbound optional.

The **ipsec direction inbound only** keyword is used when a group member wants to change a previously set IPsec SA status to inbound only.

The **ipsec direction both** keyword is used when a group member has to change a previously set IPsec SA status to both inbound and outbound. In this setting, the group member accepts only cipher text.

Examples

The following example shows how to determine whether a group member can accept cipher text.

On Group Member 1, configure the following:

```
crypto gdoi gm group groupexample ipsec direction inbound only
```

On Group Member 2, configure the following:

```
crypto gdoi gm group groupexample ipsec direction inbound optional
```

Then Ping Group Member 1.

Group Member 2 will have encrypted the packet and will send an encrypted packet to Group Member 1, which then decrypts that packet. If the traffic is from Group Member 1 to Group Member 2, Group Member 1 will forward the packet in clear text, and Group Member will accept it.

Related Commands

Command	Description
sa receive-only	Specifies that an IPsec SA is to be installed by a group member as "inbound only."

crypto gdoi group

To identify a Group Domain of Interpretation (GDOI) group and enter GDOI group configuration mode, use the **crypto gdoi group** command in global configuration mode. To disable a GDOI group, use the **no** form of this command.

crypto gdoi group {*group-name*}

no crypto gdoi group {*group-name*}

Syntax Description

group-name	Name of the group. The group name is limited to 80 characters.

Command Default

A GDOI group is not defined.

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

There are more options for configuring a group on a key server than there are for configuring a group member. The group is identified by an identity and by the server. If the crypto GDOI group is a group member, the address of the server is specified. If the crypto GDOI group is a key server, "server local" is specified, which indicates that this is the key server.

Examples

The following example shows how to configure a GDOI group for a key server:

```
crypto gdoi group gdoigroupname
 identity number 4444
 server local
```

The following example shows how to configure a GDOI group for a group member:

```
crypto gdoi group gdoigroupname
 identity number 3333
 server address ipv4 10.0.5.2
```

crypto identity

To configure the identity of the router with a given list of distinguished names (DNs) in the certificate of the router, use the **crypto identity** command in global configuration mode. To delete all identity information associated with a list of DNs, use the **no** form of this command.

crypto identity *name*

no crypto identity *name*

Syntax Description

name	Identity of the router, which is associated with the given list of DNs.

Defaults

If this command is not enabled, the IP address is associated with the identity of the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(20)T	Support for IPv6 was added.

Usage Guidelines

The **crypto identity** command allows you to configure the identity of a router with a given list of DNs. Thus, when used with the **dn** and **fqdn** commands, you can set restrictions in the router configuration that prevent peers with specific certificates, especially certificates with particular DNs, from having access to selected encrypted interfaces.

Note The identity of the peer must be the same as the identity in the exchanged certificate.

Examples

The following example shows how to configure a DN-based crypto map:

```
! The following is an IPSec crypto map (part of IPSec configuration). It can be used only
! by peers that have been authenticated by DN and if the certificate belongs to BigBiz.
crypto map map-to-bigbiz 10 ipsec-isakmp
 set peer 172.21.114.196
 set transform-set my-transformset
 match address 124
 identity to-bigbiz
!
crypto identity to-bigbiz
 dn ou=BigBiz
!
!
! This crypto map can be used only by peers that have been authenticated by hostname
```

```
! and if the certificate belongs to little.com.
crypto map map-to-little-com 10 ipsec-isakmp
 set peer 172.21.115.119
 set transform-set my-transformset
 match address 125
 identity to-little-com
!
crypto identity to-little-com
 fqdn little.com
!
```

Related Commands

Command	Description
crypto mib ipsec flowmib history failure size	Associates the identity of the router with the DN in the certificate of the router.
fqdn	Associates the identity of the router with the hostname that the peer used to authenticate itself.

crypto ikev2 authorization policy

To configure an IKEv2 client configuration group, use the **crypto ikev2 authorization policy** command in global configuration mode. To remove this command and all associated subcommands from your configuration, use the **no** form of this command.

crypto ikev2 authorization policy *policy-name*

nocrypto ikev2 authorization policy *policy-name*

Syntax Description

policy-name	Group definition that identifies which policy is enforced for users.

Command Default

No IKEv2 client group is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use the **crypto ikev2 authorization policy** command to specify the group for which a policy profile must be defined and the group policy information that needs to be defined or changed. You may wish to change the group policy on your router if you decide to connect to the client using a group ID that does not match the *policy-name* argument. The authorization policy is referred from the IKEv2 profile using the **aaa authorization group** command where the group name can be directly specified or derived from the remote identities using a name mangler.

If AAA authorization is configured as local, AAA derives the authorization attributes from IKEv2 client configuration group through the callback to crypto component.

After enabling this command, which puts the networking device in IKEv2 group configuration mode, you can specify the characteristics for the group policy using the following commands:

- **dhcp**—Configures an IP address on the remote access client for the Dynamic Host Configuration Protocol (DHCP) to use.
- **dns**—Specifies the primary and secondary Domain Name Service (DNS) servers for the group.
- **netmask**—Subnet mask to be used by the client for local connectivity.
- **pool**—Refers to the IP local pool address used to allocate internal IP addresses to clients.
- **subnet-acl**—Configures split tunneling.
- **wins**—Specifies the primary and secondary Windows Internet Naming Service (WINS) servers for the group.

Examples

The following example shows how the client configuration group is referred from IKEv2 profile using the **aaa authorization group** command where the group name is specified directly. In this example, the policy is enforced for users that matches the group name "abc."

```
aaa new-model
aaa authorization network aaa-group-list default local
!
crypto ikev2 authorization policy
abc
  pool pool1
  dns 198.51.100.1 198.51.100.100
  wins 203.0.113.1 203.0.113.115
  dhcp server 3.3.3.3
  dhcp giaddr 192.0.2.1
  dhcp timeout 10
  netmask 255.255.255.0
  subnet-acl acl-123
!
crypto ikev2 profile profile1
  authentication remote eap
aaa authorization group aaa-group-list abc
!
ip access-list extended acl-123
permit ip 209.165.200.225 0.0.0.31 any
permit ip 209.165.201.1 255.255.255.224 any
```

Related Commands

Command	Description
aaa authorization group	Sets parameters that restrict user access to a network.
dhcp	Configures an IP address for the DHCP to use.
dns	Specifies the primary and secondary DNS servers for the group.
netmask	Specifies the netmask of the subnet address that is assigned to the client.
pool	Defines a local pool address for assigning IP addresses.
subnet-acl	Defines ACL for split tunneling.
wins	Specifies the internal WINS server addresses.

crypto ikev2 certificate-cache

To set the cache size to store certificates, use the **crypto ikev2 certificate-cache** command in global configuration mode. To delete the cache size, use the **no** form of this command.

crypto ikev2 certificate-cache *number-of-certificates*

no crypto ikev2 certificate-cache

Syntax Description

number-of-certificates	The maximum number of certificates that can be stored in the cache.

Command Default

The cache size is not set.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to set the cache to store the maximum number of certificates fetched from the HTTP URLs.

Examples

The following example sets the cache size to store 500 certificates:

```
Router(config)# crypto ikev2 certificate-cache 500
```

Related Commands

Command	Description
crypto ikev2 cookie-challenge	Enables IKEv2 cookie challenge.
crypto ikev2 diagnose error	Enables IKEv2 error diagnosis.
crypto ikev2 dpd	Defines DPD globally for all peers.
crypto ikev2 http-url cert	Enables HTTP CERT support.
crypto ikev2 limit	Defines call admission control for all peers.
crypto ikev2 nat	Defines NAT keepalive globally for all peers.
crypto ikev2 window	Specifies the IKEv2 window size.
crypto logging ikev2	Enables IKEv2 syslog messages on a server.

crypto ikev2 cookie-challenge

To enable a cookie challenge for Internet Key Exchange Version 2 (IKEv2), use the **crypto ikev2 cookie-challenge** command in global configuration mode. To disable the cookie challenge, use the **no** form of this command.

crypto ikev2 cookie-challenge *number*

no crypto ikev2 cookie-challenge

Syntax Description

number	Enables the IKEv2 cookie challenge when the number of half-open security associations (SAs) crosses the configured number. The range is 1 to 1000.

Command Default

The cookie challenge is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to enable the IKEv2 cookie challenge. A cookie challenge mitigates the effect of a DoS attack when an IKEv2 responder is flooded with session initiation requests from forged IP addresses.

Examples

The following example sets the cookie challenge to 450:

```
Router(config)# crypto ikev2 cookie-challenge 450
```

Related Commands

Command	Description
crypto ikev2 certificate-cache	Specifies the cache size to store certificates fetched from HTTP URLs.
crypto ikev2 diagnose error	Enables IKEv2 error diagnosis.
crypto ikev2 dpd	Defines DPD globally for all peers.
crypto ikev2 http-url cert	Enables HTTP CERT support.
crypto ikev2 limit	Defines call admission control for all peers.
crypto ikev2 nat	Defines NAT keepalive globally for all peers.

Command	Description
crypto ikev2 window	Specifies the IKEv2 window size.
crypto logging ikev2	Enables IKEv2 syslog messages on a server.

crypto ikev2 diagnose

To enable Internet Key Exchange Version 2 (IKEv2) error diagnostics, use the **crypto ikev2 diagnose** command in global configuration mode. To disable the error diagnostics, use the **no** form of this command.

crypto ikev2 diagnose error *number*

no crypto ikev2 diagnose error

Syntax Description

error	Enables the IKEv2 error path tracing.
number	Specifies the maximum number of errors allowed in the exit path entry. The range is 1 to 1000.

Command Default

IKEv2 error diagnostics is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to enable IKEv2 error path tracing and to specify the number of entries in the exit path database. When the number exceeds the specified number, new entries replace the old entries.

Examples

The following example sets the maximum number of entries that can be logged:

```
Router(config)# crypto ikev2 diagnose error 500
```

Related Commands

Command	Description
crypto ikev2 certificate-cache	Specifies the cache size to store certificates fetched from HTTP URLs.
crypto ikev2 cookie-challenge	Enables IKEv2 cookie challenge.
crypto ikev2 dpd	Defines DPD globally for all peers.
crypto ikev2 http-url cert	Enables HTTP CERT support.
crypto ikev2 limit	Defines call admission control for all peers.
crypto ikev2 nat	Defines NAT keepalive globally for all peers.

Command	Description
crypto ikev2 window	Specifies the IKEv2 window size.
crypto logging ikev2	Enables IKEv2 syslog messages on a server.

crypto ikev2 dpd

To configure Dead Peer Detection (DPD) for Internet Key Exchange Version 2 (IKEv2), use the **crypto ikev2 dpd** command in global configuration mode. To delete DPD, use the **no** form of this command.

crypto ikev2 dpd *interval retry-interval* {**on-demand** | **periodic**}

no crypto ikev2 dpd

Syntax Description

interval	Specifies the keepalive interval in seconds.
retry-interval	Specifies the retry interval in seconds when there is no reply from the peer.
on-demand	Specifies the on-demand mode to send keepalive only in the absence of any incoming data traffic, to check the liveness of the peer before sending any data.
periodic	Specifies the periodic mode to send keepalives regularly at a specified interval.

Command Default

DPD is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to configure DPD globally for all peers. The DPD configuration in a Internet Key Exchange Version 2 (IKEv2) profile overrides the global DPD configuration.

Examples

The following example shows how to configure the periodic mode for DPD:

```
Router(config)# crypto ikev2 dpd 500 50 periodic
```

Related Commands

Command	Description
crypto ikev2 certificate-cache	Specifies the cache size to store certificates fetched from HTTP URLs.
crypto ikev2 cookie-challenge	Enables IKEv2 cookie challenge.
crypto ikev2 diagnose error	Enables IKEv2 error diagnosis.

Command	Description
crypto ikev2 http-url cert	Enables HTTP CERT support.
crypto ikev2 limit	Defines call admission control for all peers.
crypto ikev2 nat	Defines NAT keepalive globally for all peers.
crypto ikev2 window	Specifies the IKEv2 window size.
crypto logging ikev2	Enables IKEv2 syslog messages on a server.

crypto ikev2 fragmentation

To configure Internet Key Exchange Version 2 (IKEv2) fragmentation, use the **crypto ikev2 fragmentation** command in global configuration mode. To disable the fragmentation, use the **no** form of this command.

crypto ikev2 fragmentation mtu *mtu-size*

no crypto ikev2 fragmentation

Syntax Description

mtu *mtu size*	Specifies the maximum transmission unit in bytes. The range is from 68 to 1500 bytes. **Note** The MTU size refers to the IP or UDP encapsulated IKEv2 packets.

Command Default

IKEv2 fragmentation is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to fragment the IKEv2 packets at IKEv2 layer and to avoid fragmentation after encryption.

Examples

The following example shows how to configure IKEv2 fragmentation:

```
Router# enable
Router(config)# crypto ikev2 fragmentation mtu 200
```

crypto ikev2 http-url

To enable lookup based on HTTP URL, use the **crypto ikev2 http-url** command in global configuration mode. To disable the lookup based on HTTP URL, use the **no** form of this command.

crypto ikev2 http-url cert

no crypto ikev2 http-url cert

Syntax Description

cert	Enable certificate lookup based on the HTTP URL.

Command Default

HTTP CERT is enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1.(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to enable certificate lookup based on the HTTP URL. HTTP CERT indicates that the node is capable of looking up certificates based on the URL. This avoids the fragmentation that results when transferring large certificates.

Examples

The following example shows how to configure HTTP CERT:

```
Router(config)# crypto ikev2 http-url cert
```

Related Commands

Command	Description
crypto ikev2 certificate-cache	Specifies the cache size to store certificates fetched from HTTP URLs.
crypto ikev2 cookie-challenge	Enables IKEv2 cookie challenge.
crypto ikev2 diagnose error	Enables IKEv2 error diagnosis.
crypto ikev2 dpd	Defines DPD globally for all peers.
crypto ikev2 limit	Defines call admission control for all peers.
crypto ikev2 nat	Defines NAT keepalive globally for all peers.
crypto ikev2 window	Specifies the IKEv2 window size.
crypto logging ikev2	Enables IKEv2 syslog messages on a server.

crypto ikev2 keyring

To configure an Internet Key Exchange version 2 (IKEv2) key ring, use the **crypto ikev2 keyring** command in the global configuration mode. To delete an IKEv2 keyring, use the **no** form of this command.

crypto ikev2 keyring *keyring-name*

no crypto ikev2 keyring *keyring-name*

Syntax Description

keyring-name	Name of the keyring.

Command Default

There is no default key ring.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

IKEv2 keyrings are independent of IKEv1 keyrings. The key differences are as follows:

- IKEv2 keyrings support symmetric and asymmetric preshared keys.
- IKEv2 keyrings do not support Rivest, Shamir and Adleman (RSA) public keys.
- IKEv2 keyrings are specified in the IKEv2 profile and are not looked up, unlike IKEv1 where keys are looked up on receipt of MM1 to negotiate the preshared key authentication method. The authentication method is not negotiated in IKEv2.
- IKEv2 keyrings are not associated with VPN routing and forwarding (VRF) during configuration. The VRF of an IKEv2 keyring is the VRF of the IKEv2 profile that refers the keyring.
- A single keyring can be specified in an IKEv2 profile, unlike an IKEv1 profile, which can specify multiple keyrings.
- A single keyring can be specified in more than one IKEv2 profile, if the same keys are shared across peers matching different profiles.
- An IKEv2 keyring is structured as one or more peer subblocks.

On an IKEv2 initiator, IKEv2 keyring key lookup is performed using the peer's hostname or the address, in that order. Use the **hostname** (ikev2 keyring) and **address** (ikev2 keyring) commands to configure the hostname and address in the IKEv2 keyring peer configuration mode.

On an IKEv2 responder, the key lookup is performed using the peer's IKEv2 identity or the address, in that order. Use the **address** (ikev2 keyring) and **identity** (ikev2 keyring) command to configure the address and identity in IKEv2 keyring peer configuration mode.

Note You cannot configure the same identity in more than one peer.

The best match is only performed for address configurations and a key lookup is performed for the remaining peer identification, including identity address.

Examples

The following example shows how to configure a keyring:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# description example.com
Router(config-ikev2-keyring-peer)# address 0.0.0.0 0.0.0.0
Router(config-ikev2-keyring-peer)# pre-shared-key xyz-key
```

The following example shows how a keyring match is performed. In the example, the key lookup for peer 10.0.0.1 would first match the wildcard key abc-key, then the prefix key abc-key and finally the host key host1-abc-key and the best match host1-abc-key is used.

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# description example.com
Router(config-ikev2-keyring-peer)# address 0.0.0.0 0.0.0.0
Router(config-ikev2-keyring-peer)# pre-shared-key xyz-key

Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# description abc.example.com
Router(config-ikev2-keyring-peer)# address 10.0.0.0 255.255.0.0
Router(config-ikev2-keyring-peer)# pre-shared-key abc-key

Router(config-ikev2-keyring)# peer host1
Router(config-ikev2-keyring-peer)# description host1@abc.example.com
Router(config-ikev2-keyring-peer)# address 10.0.0.1
Router(config-ikev2-keyring-peer)# pre-shared-key host1-abc-key
```

In the following example, the key lookup for peer 10.0.0.1 would first match the host key host1-abc-key. Because, this is a specific match, no further lookup is performed.

```
Router(config)# crypto ikev2 keyring keyring-2
Router(config-ikev2-keyring)# peer host1
Router(config-ikev2-keyring-peer)# description host1 in abc.example.com sub-domain
Router(config-ikev2-keyring-peer)# address 10.0.0.1
Router(config-ikev2-keyring-peer)# pre-shared-key host1-abc-key

Router(config-ikev2-keyring)# peer host2
Router(config-ikev2-keyring-peer)# description example domain
Router(config-ikev2-keyring-peer)# address 0.0.0.0 0.0.0.0
Router(config-ikev2-keyring-peer)# pre-shared-key xyz-key
```

Related Commands

Command	Description
address (ikev2 keyring)	Specifies the IPv4 address or the range of the peers in IKEv2 keyring.
description (ikev2 keyring)	Describes an IKEv2 peer or a peer group for the IKEv2 keyring.
hostname (ikev2 keyring)	Specifies the hostname for the peer in the IKEv2 keyring.

Command	Description
identity (ikev2 keyring)	Identifies the peer with IKEv2 types of identity.
peer	Defines a peer or a peer group for the keyring.
pre-shared-key (ikev2 keyring)	Defines a preshared key for the IKEv2 peer.

crypto ikev2 limit

To enable call admission control in Internet Key Exchange Version 2 (IKEv2), use the **crypto ikev2 limit** command in global configuration mode. To disable call admission control, use the **no** form of this command.

crypto ikev2 limit {**max-in-negotiation-sa** | **max-sa**} *limit*

no crypto ikev2 limit {**max-in-negotiation-sa** | **max-sa**}

Syntax Description

max-in-negotiation-sa	Limits the total number of in-negotiation IKEv2 security associations (SAs) on the node.
max-sa	Limits the total number of IKEv2 SAs on the node.

Command Default

There is no configured limit on the number of IKEv2 SAs by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Call admission control limits the in-negotiation and total number of IKEv2 SA on a node.

Note In IKEv2, rekey is not a new security association (SA) unlike in IKEv1. Hence, the rekey SA is not counted.

Examples

The following example shows how to enable call admission control:

```
Router(config)# crypto ikev2 max-in-negotiation-sa limit 5000
```

Related Commands

Command	Description
crypto ikev2 certificate-cache	Specifies the cache size to store certificates fetched from HTTP URLs.
crypto ikev2 cookie-challenge	Enables IKEv2 cookie challenge.
crypto ikev2 diagnose error	Enables IKEv2 error diagnosis.

Command	Description
crypto ikev2 dpd	Defines DPD globally for all peers.
crypto ikev2 http-url cert	Enables HTTP CERT support.
crypto ikev2 nat	Defines NAT keepalive globally for all peers.
crypto ikev2 window	Specifies the IKEv2 window size.
crypto logging ikev2	Enables IKEv2 syslog messages on a server.

crypto ikev2 name mangler

To configure the Internet Key Exchange version 2 (IKEv2) name mangler, use the **crypto ikev2 name mangler** command in global configuration mode. To delete the name mangler, use the **no** form of this command.

crypto ikev2 name mangler *mangler-name*

no crypto ikev2 name mangler *mangler-name*

Syntax Description

mangler-name	IKEv2 mangler name.

Command Default

IKEv2 name mangler is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

The IKEv2 name mangler is used to derive a name for the AAA group or user authorization requests. The name mangler contains multiple statements—one for each identity type. The name mangler is derived from the specified portions of different forms of remote IKE identities or EAP identity. The name mangler is referred in the IKEv2 profile using the **aaa authorization** command.

After enabling this command, which puts the networking device in IKEv2 name mangler configuration mode, you can specify the characteristics for the name mangler using the following commands:

- **dn**—Derives the name from the remote identity of type distinguished name (DN).
- **eap**—Derives the name from remote identities of type Extensible Authentication Protocol (EAP).
- **email**—Derives the name from the remote identity of type e-mail.
- **fqdn**—Derives the name from the remote identity of type Fully Qualified Domain Name (FQDN).

Examples

The following example shows how to define name manglers based on identity of type FQDN:

```
crypto ikev2 name-mangler mangler1
 fqdn domain

crypto ikev2 name-mangler mangler2
 fqdn hostname

crypto ikev2 name-mangler mangler3
 fqdn all
```

The following example shows how to define name manglers based on identity of type e-mail:

```
crypto ikev2 name-mangler mangler1
 email domain

crypto ikev2 name-mangler mangler2
 email username

crypto ikev2 name-mangler mangler3
 email all
```

The following example shows how to define name manglers based on identity of type DN:

```
crypto ikev2 name-mangler mangler2
  DN country

crypto ikev2 name-mangler mangler3
  DN state

crypto ikev2 name-mangler mangler4
  DN organization

crypto ikev2 name-mangler mangler5
  DN organization-unit
```

The following example shows how to define name manglers based on identity of type EAP:

```
crypto ikev2 name-mangler mangler1
  eap all

crypto ikev2 name-mangler mangler2
  eap prefix user123 delimiter @

crypto ikev2 name-mangler mangler3
  eap suffix cisco delimiter

crypto ikev2 name-mangler mangler4
 eap DN common-name
```

Related Commands

Command	Description
dn (IKEv2)	Derives the name from identity of type DN.
eap (IKEv2)	Derives the name from identity of type EAP.
email	Derives the name from identity of type e-mail.
fqdn	Derives the name from identity of type FQDN.

crypto ikev2 nat

To configure Network Address Translation (NAT) keepalive for Internet Key Exchange Version 2 (IKEv2), use the **crypto ikev2 nat** command in global configuration mode. To delete NAT keepalive configuration, use the **no** form of this command.

crypto ikev2 nat keepalive *interval*

no crypto ikev2 nat keepalive *interval*

Syntax Description

keepalive *interval*	Specifies the NAT keepalive interval in seconds.

Command Default

NAT keepalive is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to configure NAT keepalive globally for all peers. The NAT keepalive configuration specified in the IKEv2 profile overrides the global configuration. NAT keepalive prevents the deletion of NAT translation entries in the absence of any traffic, when NAT is between IKEv2 peers.

Examples

The following example shows how to specify a NAT keepalive interval of 500 seconds:

```
Router(config)# crypto ikev2 nat keepalive 500
```

Related Commands

Command	Description
crypto ikev2 certificate-cache	Specifies the cache size to store certificates fetched from HTTP URLs.
crypto ikev2 cookie-challenge	Enables IKEv2 cookie challenge.
crypto ikev2 diagnose error	Enables IKEv2 error diagnosis.
crypto ikev2 dpd	Defines DPD globally for all peers.
crypto ikev2 http-url cert	Enables HTTP CERT support.
crypto ikev2 limit	Defines call admission control for all peers.

Command	Description
crypto ikev2 window	Specifies the IKEv2 window size.
crypto logging ikev2	Enables IKEv2 syslog messages on a server.

crypto ikev2 policy

To configure an Internet Key Exchange Version 2 (IKEv2) policy, use the **crypto ikev2 policy** command in global configuration mode. To delete a policy, use the **no** form of this command.

crypto ikev2 policy *name*

no crypto ikev2 policy *name*

Syntax Description

name	Name of the IKEv2 policy.

Command Default

A default IKEv2 policy is used only in the absence of any user-defined IKEv2 policy. The default IKEv2 policy will have the default IKEv2 proposal and will match all local addresses in a global VPN Routing and Forwarding (VRF).

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

An IKEv2 policy contains the proposals that are used to negotiate the encryption, integrity, Psuedo-Random Function (PRF) algorithms and Diffie-Hellman (DH) group in SA_INIT exchange. IKEv2 policy can have match statements, which are used as selection criteria to select a policy for negotiation.

An IKEv2 policy must contain at least one proposal to be considered as complete, and can have more proposals and match statements.

A policy can have similar or different match statements. Match statements that are similar are logically ORed and match statements that are different are logically ANDed. There is no precedence between match statements of different types. If there are policies with similar match statements, the first policy configured is selected. If there are policies with overlapping match statements, the policy with the best or most specific match is selected.

A policy is matched as follows:

- If no IKEv2 policy is configured, the default policy is used for negotiating a SA that uses any local address in a global VRF.
- If IKEv2 policies are configured, the policy with the best match is selected.
- If none of the configured policies matches, the SA_INIT exchange does not start.

Examples

The following examples show how to configure a policy and how a policy match is performed:

```
Router(config)# crypto ikev2 policy policy1
Router(config-ikev2-policy)# proposal pro1
Router(config-ikev2-policy)# match fvrf green
Router(config-ikev2-policy)# match address local 10.0.0.1
```

The policy policy1 is selected and proposal pro1 is used for negotiating IKEv2 SA with the local address as 10.0.0.1 and the FVRF as green:

```
Router(config)# crypto ikev2 policy policy1
Router(config-ikev2-policy)# proposal pro1
Router(config-ikev2-policy)# match address local 10.0.0.1
```

The policy policy1 is selected and proposal pro1 is used for negotiation of the IKEv2 SA that is negotiatied with the local address as 10.0.0.1 and the FVRF as global:

```
Router(config)# crypto ikev2 policy policy1
Router(config-ikev2-policy)# proposal pro1
Router(config-ikev2-policy)# match fvrf green
```

The policy policy1 is selected and proposal pro1 is used for negotiation of the IKEv2 SA that is negotiatied with any local address and the FVRF as green.

How a Policy Match Is Performed

The following example shows how a policy is chosen out of two policies:

```
Router(config)# crypto ikev2 policy policy1
Router(config-ikev2-policy)# proposal1
Router(config-ikev2-policy)# match fvrf green

Router(config)# crypto ikev2 policy policy2
Router(config-ikev2-policy)# proposal1
Router(config-ikev2-policy)# match fvrf green
Router(config-ikev2-policy)# match local address 10.0.0.1
```

To negotiate the SA for local address 10.0.0.1 and FVRF as green, policy 2 is selected because policy 2 is the best match:

```
Router(config)# crypto ikev2 policy policy1
Router(config-ikev2-policy)# proposal2
Router(config-ikev2-policy)# match local address 10.0.0.1
Router(config-ikev2-policy)# match fvrf green

Router(config)# crypto ikev2 policy policy2
Router(config-ikev2-policy)# proposal1
Router(config-ikev2-policy)# match fvrf green
Router(config-ikev2-policy)# match local address 10.0.0.1
```

In this case, even though both the policies are the best match, policy1 is selected, because it was configured first.

Related Commands

Command	Description
match (ikev2 policy)	Matches an IKEv2 policy based on the parameters.
proposal	Specifies the proposals that must be used in the IKEv2 policy.
show crypto ikev2 policy	Displays the default or user-defined IKEv2 policy.

crypto ikev2 profile

To configure an Internet Key Exchange Version 2 (IKEv2) profile, use the **crypto ikev2 profile** command in global configuration mode. To delete the profile, use the **no** form of this command.

crypto ikev2 profile *profile-name*

no crypto ikev2 profile *profile-name*

Syntax Description

profile-name	Name of the IKEv2 profile.

Command Default

There is no default IKEv2 profile. However, there are default values for some commands under the profile, such as lifetime.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to define an IKEv2 profile. An IKEv2 profile is a repository of the nonnegotiable parameters of the IKE security associations (SAs) (such as local/remote identities and authentication methods) and the services that will be available to the authenticated peers that match the profile. The following are the characteristics of an IKEv2 profile:

- It must be attached to either a crypto map or an IPsec profile on the IKEv2 initiator and responder.
- It must contain a match identity or match certificate statement; otherwise the profile is considered incomplete and is unused.
- The statements match VRF, local or remote authentication methods are optional.

Table 21 describes the differences between IKEv1 and IKEv2 profiles.

Table 21 Differences between IKEv1 and IKEv2 Profiles

IKEv1	IKEv2
The authentication method is a negotiable parameter and must be specified in the ISAKMP policy.	The authentication method is not a negotiable parameter, can be asymmetric, and must be specified in the profile.
Multiple keyrings can be specified in the profile.	A single keyring can be specified in the profile and is optional also.

The IKEv2 profile applied on the crypto interface must be the same as IKEv2 profile that matches the peer identity received in the IKE_AUTH exchange.

Examples

The following examples show an IKEv2 profile matched on a remote identity and an IKEv2 profile catering to two peers using different authentication method.

IKEv2 Profile Matched on Remote Identity

The following profile caters to peers that identify using fqdn example.com and authenticate with rsa-signature using trustpoint-remote. The local node authenticates with pre-share using keyring-1.

```
Router(config)# crypto ikev2 profile profile2
Router(config-ikev2-profile)# match identity remote fqdn example.com
Router(config-ikev2-profile)# identity local email router2@example.com
Router(config-ikev2-profile)# authentication local pre-share
Router(config-ikev2-profile)# authentication remote rsa-sig
Router(config-ikev2-profile)# keyring keyring-1
Router(config-ikev2-profile)# pki trustpoint trustpoint-remote verify
Router(config-ikev2-profile)# lifetime 300
Router(config-ikev2-profile)# dpd 5 10 on-demand
Router(config-ikev2-profile)# virtual-template 1
```

IKEv2 Profile Catering to Two Peers Using Different Authentication Method

The following profile caters to two peers: user1@example.com that authenticate with pre-share using keyring-1, and user2@example.com authenticates with rsa-signature using trustpoint-remote. However, the local peer authenticates the remote peers with rsa-signature using trustpoint-local.

```
Router(config)# crypto ikev2 profile profile2
Router(config-ikev2-profile)# match identity remote email user1@example.com
Router(config-ikev2-profile)# match identity remote email user2@example.com
Router(config-ikev2-profile)# identity local email router2@abc.com
Router(config-ikev2-profile)# authentication local rsa-sig
Router(config-ikev2-profile)# authentication remote pre-share
Router(config-ikev2-profile)# authentication remote rsa-sig
Router(config-ikev2-profile)# keyring keyring-1
Router(config-ikev2-profile)# pki trustpoint trustpoint-local sign
Router(config-ikev2-profile)# pki trustpoint trustpoint-remote verify
Router(config-ikev2-profile)# lifetime 300
Router(config-ikev2-profile)# dpd 5 10 on-demand
Router(config-ikev2-profile)# virtual-template 1
```

EAP Authentication with External EAP Server

The following example shows how to configure the remote access server using the remote EAP authentication method with an external EAP server:

```
aaa new-model
aaa authentication login aaa-eap-list default group radius
!
crypto ikev2 profile profile2
 authentication remote eap
 aaa authentication eap aaa-eap-list
```

EAP Authentication with Local and External EAP

The following example shows how to configure the remote access server with local and external EAP server using the remote EAP authentication method:

```
aaa new-model
aaa authentication login aaa-eap-list default group radius
aaa authentication login aaa-eap-local-list default group tacacs
```

```
!
crypto ikev2 profile profile2
 authentication remote eap
 authentication remote eap-local
 aaa authentication eap aaa-eap-list
 aaa authentication eap-local aaa-eap-local-list
```

Configuring the Local Policy

This example shows how to configure the AAA authorization for a local group policy:

```
aaa new-model
aaa authorization network aaa-group-list default local
!
 crypto ikev2 client configuration group cisco
  pool addr-pool1
  dns 198.51.100.1 198.51.100.100
  wins 203.0.113.1 203.0.113.115
 !
 crypto ikev2 profile profile1
  authentication remote eap
  aaa authorization group aaa-group-list abc
```

The aaa-group-list specifies that the group authorization is local and that the AAA username is abc. The authorization list name corresponds to the group policy defined in the **crypto ikev2 client configuration group** command.

External AAA-based Group Policy

This example shows how to configure an external AAA-based group policy. The aaa-group-list specifies that the group authorization is RADIUS based. The name mangler derives the group name from the domain part of ID-FQDN, which is abc.

```
 aaa new-model
 aaa authorization network aaa-group-list default group radius
 !
 crypto ikev2 name-mangler mangler1
  fqdn domain
  !
 crypto ikev2 profile profile1
  identity remote fqdn host1.abc
  authentication remote eap
  aaa authorization group aaa-group-list name-mangler mangler1
```

External AAA-based User Policy

This example shows how to configure an external AAA-based group policy. The aaa-user-list specifies that the user authorization is RADIUS based. The name mangler derives the username from the hostname part of ID-FQDN, which is host1.

```
aaa new-model
aaa authorization network aaa-user-list default group radius
!
crypto ikev2 name-mangler mangler2
 fqdn hostname
!
crypto ikev2 profile profile1
 match identity remote fqdn host1.abc
  authentication remote eap
 aaa authorization user aaa-user-list name-mangler mangler2
```

Related Commands

Command	Description
aaa authentication (IKEv2 profile)	Defines the AAA authentication list for EAP authentication.
aaa authorization (IKEv2 profile)	Defines the AAA authorization for a local or group policy.
authentication (IKEv2 profile)	Defines the local and remote authentication methods.
crypto ikev2 keyring	Defines an IKEv2 keyring.
show crypto ikev2 profile	Displays the IKEv2 profile.

crypto ikev2 proposal

To configure an Internet Key Exchange Version 2 (IKEv2) proposal, use the **crypto ikev2 proposal** command in global configuration mode. To delete an IKEv2 proposal, use the **no** form of this command.

crypto ikev2 proposal *name*

no crypto ikev2 proposal *name*

Syntax Description

name	Name of the proposal. The proposals are attached to IKEv2 policies using the **proposal** command.

Command Default

The default IKEv2 proposal is used.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

An IKEv2 proposal is a set of transforms used in the negotiation of IKEv2 SA as part of the IKE_SA_INIT exchange. An IKEv2 proposal is regarded as complete only when it has at least an encryption algorithm, an integrity algorithm and a Diffie-Hellman (DH) group configured. If no proposal is configured and attached to an IKEv2 policy, then the default proposal is used in negotiation. The default proposal is a collection of commonly used algorithms, which are as follows:

```
encryption aes-cbc-128 3des
integrity sha md5
group 5 2
```

The transforms shown translate to the following combinations in the following order of priority:

```
aes-cbc-128, sha, 5
aes-cbc-128, sha, 2
aes-cbc-128, md5, 5
aes-cbc-128, md5, 2
3des, sha, 5
3des, sha, 2
3des, md5, 5
3des, md5, 2
```

Although this command is similar to the **crypto isakmp policy** command, the IKEv2 proposal differs as follows:

- An IKEv2 proposal allows configuration of one or more transforms for each transform type.
- An IKEv2 proposal does not have any associated priority.

Note The IKEv2 proposals must be attached to the IKEv2 policies for using the proposals in negotiation. If a proposal is not configured, then the default IKEv2 proposal is used with the default IKEv2 policy.

When multiple transforms are configured for a transform type, the order of priority is from left to right.

A proposal with multiple transforms for each transform type translates to all possible combinations of transforms. If only a subset of these combinations is required, then they must be configured as individual proposals.

```
Router(config)# crypto ikev2 proposal proposal-1
Router(config-ikev2-proposal)# encryption 3des, aes-cbc-128
Router(config-ikev2-proposal)# integrity sha, md5
Router(config-ikev2-proposal)# group 2
```

For example, the commands shown translates to the following transform combinations:

```
3des, sha, 2
aes-cbc-128, sha, 2
3des, md5, 2
aes-cbc-128, md5, 2
```

To configure the first and last transform combinations, the commands are as follows:

```
Router(config)# crypto ikev2 proposal proposal-1
Router(config-ikev2-proposal)# encryption 3des
Router(config-ikev2-proposal)# integrity sha
Router(config-ikev2-proposal)# group 2

Router(config)# crypto ikev2 proposal proposal-2
Router(config-ikev2-proposal)# encryption aes-cbc-128
Router(config-ikev2-proposal)# integrity md5
Router(config-ikev2-proposal)# group 2
```

Examples

The following examples show how to configure a proposal:

IKEv2 Proposal with One Transform for Each Transform Type

```
Router(config)# crypto ikev2 proposal proposal-1
Router(config-ikev2-proposal)# encryption 3des
Router(config-ikev2-proposal)# integrity sha
Router(config-ikev2-proposal)# group 2
```

IKEv2 Proposal with Multiple Transforms for Each Transform Type

```
Router(config)# crypto ikev2 proposal proposal-2
Router(config-ikev2-proposal)# encryption 3des aes-cbc-128
Router(config-ikev2-proposal)# integrity sha md5
Router(config-ikev2-proposal)# group 2 5
```

The IKEv2 proposal **proposal-2** shown translates to the following prioritized list of transform combinations:

- 3des, sha, 2
- 3des, sha, 5
- 3des, md5, 2
- 3des, md5, 5
- aes-cbc-128, sha, 2

- aes-cbc-128, sha, 5
- aes-cbc-128, md5, 2
- aes-cbc-128, md5, 5

IKEv2 Proposals on the Initiator and Responder

The proposal of the initiator is as follows:

```
Router(config)# crypto ikev2 proposal proposal-1
Router(config-ikev2-proposal)# encryption 3des aes-cbc-128
Router(config-ikev2-proposal)# integrity sha md5
Router(config-ikev2-proposal)# group 2 5
```

The proposal of the responder is as follows:

```
Router(config)# crypto ikev2 proposal proposal-2
Router(config-ikev2-proposal)# encryption aes-cbc-128 3des
Router(config-ikev2-proposal)# integrity md5 sha
Router(config-ikev2-proposal)# group 5 2
```

In the scenario shown, the initiator choice of algorithms is preferred and the selected algorithms are as follows:

```
encryption 3des
integrity sha
group 2
```

Related Commands

Command	Description
encryption (ikev2 proposal)	Specifies the encryption algorithm in an IKEv2 proposal.
group (ikev2 proposal)	Specifies the Diffie-Hellman group identifier in an IKEv2 proposal.
integrity (ikev2 proposal)	Specifies the integrity algorithm in an IKEv2 proposal.
show crypto ikev2 proposal	Displays the parameters for each IKEv2 proposal.

crypto ikev2 window

To configure the Internet Key Exchange Version 2 (IKEv2) window size, use the **crypto ikev2 window** command in global configuration mode. To delete IKEv2 window configuration, use the **no** form of this command.

crypto ikev2 window *window-size*

no crypto ikev2 window

Syntax Description

window-size	Size of the window that can range from 1 to 20.

Command Default

The default window size is 5.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Window size allows multiple IKEv2 request-response pairs in transit. Use this command to specify the IKEv2 window size to have multiple IKEv2 request-response pairs in transit.

Examples

The following example shows how to configure a window size of 10:

```
Router(config)# crypto ikev2 window size 10
```

Related Commands

Command	Description
crypto ikev2 certificate-cache	Specifies the cache size to store certificates fetched from HTTP URLs.
crypto ikev2 cookie-challenge	Enables IKEv2 cookie challenge.
crypto ikev2 diagnose error	Enables IKEv2 error diagnosis.
crypto ikev2 dpd	Defines DPD globally for all peers.
crypto ikev2 http-url cert	Enables HTTP CERT support.
crypto ikev2 limit	Defines call admission control for all peers.

Command	Description
crypto ikev2 nat	Defines NAT keepalive globally for all peers.
crypto logging ikev2	Enables IKEv2 syslog messages on a server.

crypto ipsec client ezvpn (global)

To create a Cisco Easy VPN remote configuration and enter the Cisco Easy VPN remote configuration mode, use the **crypto ipsec client ezvpn** command in global configuration mode. To delete the Cisco Easy VPN remote configuration, use the **no** form of this command.

crypto ipsec client ezvpn *name*

no crypto ipsec client ezvpn *name*

Note A separate **crypto ipsec client ezvpn** command in interface configuration mode assigns a Cisco Easy VPN remote configuration to the interface.

Syntax Description

name	Identifies the Cisco Easy VPN remote configuration with a unique, arbitrary name.

Command Default

Newly created Cisco Easy VPN remote configurations default to client mode.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(4)YA	This command was introduced for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(8)YJ	This command was enhanced to enable you to manually establish and terminate an IPsec VPN tunnel on demand for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(4)T	The **username** command was added, and the **pee**command was changed so that the command may now be input multiple times.
12.3(7)XR	The **acl** and **backup** commands were added.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.3(11)T	The **acl** command was integrated into Cisco IOS Release 12.3(11)T. However, the **backup** command was not integrated into Cisco IOS Release 12.3(11)T.
12.4(2)T	The **virtual-interface** command was added.
12.4(4)T	The **default** keyword was added to the **peer** command, and the **flow allow acl** and **idle-time** commands were added.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The **nat acl** and **nat allow** commands were added.

Usage Guidelines

The **crypto ipsec client ezvpn** command creates a Cisco Easy VPN remote configuration and then enters the Cisco Easy VPN remote configuration mode, at which point you can enter the following commands:

- **acl** {*acl-name* | *acl-number*}—Specifies multiple subnets in a Virtual Private Network (VPN) tunnel. Up to 50 subnets may be configured.
  - The *acl-name* argument is the name of the access control list (ACL).
  - The *acl-number* argument is the number of the ACL.

Note Use the **acl** command in the Network Extension Mode (NEM) to expand the networks that are being extended. The **permit** statements in the ACL allow you to add additional networks to the list of extended networks. Without an ACL, the VPN only provides connectivity with the directly connected network of the inside interface.

- **backup** {*ezvpn-config-name*} **track** {*tracked-object-number*}—Specifies the Easy VPN configuration that will be activated when the backup is triggered.
  - **backup** {*ezvpn-config-name*}—Specifies the Easy VPN configuration that will be activated when the backup is triggered.
  - **track** {*tracked-object-number*}—Specifies the link to the tracking system so that the Easy VPN state machine can get the notification to trigger the backup.
- **connect** [**auto** | **manual** | **acl**]—Manually establishes and terminates an IP Security (IPsec) tunnel on demand.
  - The **auto** keyword is the default setting, because it was the initial Cisco Easy VPN remote functionality. The IPsec VPN tunnel is automatically connected when the Cisco Easy VPN Remote feature is configured on an interface.
  - The **manual** keyword specifies the manual setting to direct the Cisco Easy VPN remote to wait for a command or application programming interface (API) call before attempting to establish the Cisco Easy VPN remote connection. When the tunnel times out or fails, subsequent connections have to wait for the command to reset to manual or to an API call.
  - The **acl** keyword specifies the ACL-triggered setting, which is used for transactional-based applications and dial backup. Using this option, you can define the "interesting" traffic that triggers the tunnel to be established.
- **default**—Sets the following command to its default values.
- **exit**—Exits the Cisco Easy VPN configuration mode and returns to global configuration mode.
- **flow allow acl** [*name* | *number*]—Restricts the client from sending traffic in clear text when the tunnel is down. The *name* argument is the access list name. The *number* argument is the access list number, which can be 100 through 199.
- **group** *group-name* **key** *group-key*—Specifies the group name and key value for the VPN connection.
- **idletime**—(Optional) Sets the idle time after which an Easy VPN tunnel is brought down.

- **local-address** *interface-name*—Informs the Cisco Easy VPN remote which interface is used to determine the public IP address, which is used to source the tunnel. This command applies only to the Cisco uBR905 and Cisco uBR925 cable access routers.
  - The value of the *interface-name* argument specifies the interface used for tunnel traffic.

  After specifying the local address used to source tunnel traffic, the IP address can be obtained in two ways:
  - The **local-address** command can be used with the **cable-modem dhcp-proxy** {**interface loopback** *number*} command to obtain a public IP address and automatically assign it to the loopback interface.
  - The IP address can be manually assigned to the loopback interface.
- **mode** {**client | network-extension | network extension plus**}—Specifies the VPN mode of operation of the router:
  - The **client** keyword (default) automatically configures the router for Cisco Easy VPN client mode operation, which uses Network Address Translation (NAT) or Peer Address Translation (PAT) address translations. When the Cisco Easy VPN remote configuration is assigned to an interface, the router automatically creates the NAT or PAT and access list configuration needed for the VPN connection.
  - The **network-extension** keyword specifies that the router should become a remote extension of the enterprise network at the other end of the VPN connection. The PCs that are connected to the router typically are assigned an IP address in the address space of the enterprise network.
  - The **network extension plus** keyword is identical to network extension mode with the additional capability of being able to request an IP address via mode configuration and automatically assign it to an available loopback interface. The IPsec security associations (SAs) for this IP address are automatically created by Easy VPN Remote. The IP address is typically used for troubleshooting (using ping, Telnet, and Secure Shell).
- **nat acl** {*acl-name* | *acl-number*}—Enables split-tunneling for the traffic specified by the ACL name or the ACL number.
  - The *acl-name* argument is the name of the ACL.
  - The *acl-number* argument is the number of the ACL.
- nat allow—Allows NAT to be integrated with Cisco Easy VPN.
- **no**—Removes the command or sets it to its default values.
- **peer** {*ipaddress* | *hostname*} [**default**]—Sets the peer IP address or hostname for the VPN connection. A hostname can be specified only when the router has a Domain Name System (DNS) server available for hostname resolution.

  The **peer** command may be input multiple times.

  The **default** keyword defines the given peer as the primary peer. When Phase 1 SA negotiations fail and Easy VPN fails over from the primary peer to the next peer on its backup list and the primary peer is again available, the current connection is torn down and the primary peer is reconnected.
- **username** *name* **password** {**0** | **6**} {*password*}—Allows you to save your extended authentication (Xauth) password locally on the PC. On subsequent authentications, you may activate the save-password tick box on the software client or add the username and password to the Cisco IOS hardware client profile. The setting remains until the save-password attribute is removed from the server group profile.
  - **0** specifies that an unencrypted password will follow.
  - **6** specifies that an encrypted password will follow.

  - *password* specifies an unencrypted (cleartext) user password.

  The save-password option is useful only if the user password is static, that is, it is not a one-time password (OTP), such as a password generated by a token.

- **virtual-interface** [*virtual-template-number*]—Specifies a virtual interface for an Easy VPN remote device. If a virtual template number is specified, the virtual interface is derived from the virtual template that is configured. If a virtual template number is not specified, a generic virtual-access interface of the type tunnel is created. If the creation is successful, Easy VPN makes the virtual-access interface its outside interface (that is, the crypto map and NAT are applied on the virtual-access interface). If the creation is a failure, Easy VPN prints an error message and remains in the IDLE state.

After configuring the Cisco Easy VPN remote configuration, use the **exit** command to exit the Cisco Easy VPN remote configuration mode and return to global configuration mode.

Note You cannot use the **no crypto ipsec client ezvpn** command to delete a Cisco Easy VPN remote configuration that is assigned to an interface. You must remove that Cisco Easy VPN remote configuration from the interface before you can delete the configuration.

Examples

The following example shows a Cisco Easy VPN remote configuration named "telecommuter-client" being created on a Cisco uBR905 or Cisco uBR925 cable access router and being assigned to cable interface 0:

```
Router# configure terminal
Router(config)# crypto ipsec client ezvpn telecommuter-client
Router(config-crypto-ezvpn)# group telecommute-group key secret-telecommute-key
Router(config-crypto-ezvpn)# peer telecommuter-server
Router(config-crypto-ezvpn)# mode client
Router(config-crypto-ezvpn)# exit
Router(config)# interface c0
Router(config-if)# crypto ezvpn telecommuter-client
Router(config-if)# exit
```

Note Specifying the **mode client** option as shown above is optional because this is a default configuration for these options.

The following example shows the Cisco Easy VPN remote configuration named "telecommuter-client" being removed from the interface and then deleted:

```
Router# configure terminal
Router(config)# interface e1
Router(config-if)# no crypto ipsec client ezvpn telecommuter-client
Router(config-if)# exit
Router(config)# no crypto ipsec client ezvpn telecommuter-client
```

The following example shows that a virtual IPsec interface has been configured for the Easy VPN remote device:

```
crypto ipsec client ezvpn EasyVPN1
 virtual-interface 3
```

Related Commands

Command	Description
crypto ipsec client ezvpn (interface)	Assigns a Cisco Easy VPN remote configuration to an interface.

crypto ipsec client ezvpn (interface)

To assign a Cisco Easy Virtual Private Network (VPN) remote configuration to an interface other than a virtual interface, to specify whether the interface is outside or inside, and to configure multiple outside and inside interfaces, use the **crypto ipsec client ezvpn** command in interface configuration mode. To remove the Cisco Easy VPN remote configuration from the interface, use the **no** form of this command.

crypto ipsec client ezvpn *name* [**outside | inside**]

no crypto ipsec client ezvpn *name* [**outside | inside**]

Syntax Description

name	Specifies the Cisco Easy VPN remote configuration to be assigned to the interface. **Note** The interface specified cannot be a virtual interface.
outside	(Optional) Specifies the outside interface of the IP Security (IPsec) client router. You can add up to four outside tunnels for all platforms, one tunnel per outside interface.
inside	(Optional) Specifies the inside interface of the IPsec client router. The Cisco 1700 series has no default inside interface, and any inside interface must be configured. The Cisco 800 series routers and Cisco uBR905 and Cisco uBR925 cable access routers have default inside interfaces. However, you can configure any inside interface and add up to three inside interfaces for all platforms.

Defaults

The default inside interface is the Ethernet interface on Cisco 800 series routers and Cisco uBR905 and Cisco uBR925 cable access routers.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(4)YA	This command was introduced on Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(8)YJ	This command was enhanced to enable you to configure multiple outside and inside interfaces for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

The **crypto ipsec client ezvpn** command assigns a Cisco Easy VPN remote configuration to an interface, enabling the creation of a VPN connection over that interface to the specified VPN peer. If the Cisco Easy VPN remote configuration is configured for the client mode of operation, the router is also automatically configured for network address translation (NAT) or port address translation (PAT) and for an associated access list.

Note The **crypto ipsec client ezvpn** command is not supported on virtual interfaces.

Release 12.2(8)YJ

The **crypto ipsec client ezvpn** command was enhanced to allow you to configure multiple outside and inside interfaces. To configure multiple outside and inside interfaces, you must use the **interface** *interface-name* command to first define the type of interface on the IPsec client router.

- In client mode for the Cisco Easy VPN client, a single security association (SA) connection is used for encrypting and decrypting the traffic coming from all the inside interfaces. In network extension mode, one SA connection is established for each inside interface.
- When a new inside interface is added or an existing one is removed, all established SA connections are deleted and new ones are initiated.
- Configuration information for the default inside interface is shown with the **crypto ipsec client ezvpn name inside** command. All inside interfaces, whether they belong to a tunnel, are listed in interface configuration mode as an inside interface, along with the tunnel name.

Release 12.2(4)YA

The following restrictions apply to the **crypto ipsec client ezvpn** command:

- The Cisco Easy VPN remote feature supports only one tunnel, so the **crypto ipsec client ezvpn** command can be assigned to only one interface. If you attempt to assign it to more than one interface, an error message is displayed. You must use the **no** form of this command to remove the configuration from the first interface before assigning it to the second interface.
- The **crypto ipsec client ezvpn** command should be assigned to the outside interface of the NAT or PAT. This command cannot be used on the inside NAT or PAT interface. On some platforms, the inside and outside interfaces are fixed.

  For example, on Cisco uBR905 and Cisco uBR925 cable access routers, the outside interface is always the cable interface. On Cisco 1700 series routers, the FastEthernet interface defaults to being the inside interface, so attempting to use the **crypto ipsec client ezvpn** command on the FastEthernet interface displays an error message.

Note A separate **crypto ipsec client ezvpn** command exists in global configuration mode that creates a Cisco Easy VPN remote configuration.

You must first use the global configuration version of the **crypto ipsec client ezvpn** command to create a Cisco Easy VPN remote configuration before assigning it to an interface.

Examples

The following example shows a Cisco Easy VPN remote configuration named “telecommuter-client” being assigned to the cable interface on a Cisco uBR905 or a Cisco uBR925 cable access router:

```
Router# configure terminal
Router(config)# interface c0
Router(config-if)# crypto ipsec client ezvpn telecommuter-client
```

```
Router(config-if)# exit
```

The following example first shows an attempt to delete the Cisco Easy VPN remote configuration named "telecommuter-client," but the configuration cannot be deleted because it is still assigned to an interface. The configuration is then removed from the interface and deleted.

```
Router# configure terminal
Router(config)# no crypto ipsec client ezvpn telecommuter-client
Error: crypto map in use by interface; cannot delete
Router(config)# interface e1
Router(config-if)# no crypto ipsec client ezvpn telecommuter-client
Router(config-if)# exit
Router(config)# no crypto ipsec client ezvpn telecommuter-client
```

Related Commands

Command	Description
crypto ipsec client ezvpn (global)	Creates and modifies a Cisco Easy VPN remote configuration.
interface	Configures an interface type.

crypto ipsec client ezvpn connect

To connect to a specified IPSec Virtual Private Network (VPN) tunnel in a manual configuration, use the **crypto ipsec client ezvpn connect** command in privileged EXEC mode. To disable the connection, use the **no** form of this command.

crypto ipsec client ezvpn connect *name*

no crypto ipsec client ezvpn connect *name*

Syntax Description

name	Identifies the IPSec VPN tunnel with a unique, arbitrary name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)YJ	This command was introduced on Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

This command is used with the **connect** [**auto** | **manual** | **acl**] subcommand. After the manual setting is designated, the Cisco Easy VPN remote waits for a command or application programming interface (API) call before attempting to establish the Cisco Easy VPN remote connection.

If the configuration is manual, the tunnel is connected only after the **crypto ipsec client ezvpn connect** *name* command is entered in privileged EXEC mode, and after the **connect** [**auto**] | **manual** subcommand is entered.

Examples

The following example shows how to connect an IPSec VPN tunnel named ISP-tunnel on a Cisco uBR905/uBR925 cable access router:

```
Router# crypto ipsec client ezvpn connect ISP-tunnel
```

Related Commands

Command	Description
connect	Manually establishes and terminates an IPSec VPN tunnel on demand.
crypto ipsec client ezvpn (global)	Creates and modifies a Cisco Easy VPN remote configuration.

crypto ipsec client ezvpn xauth

To respond to a pending Virtual Private Network (VPN) authorization request, use the **crypto ipsec client ezvpn xauth** command in privileged EXEC mode.

crypto ipsec client ezvpn xauth *name*

Syntax Description

name	Identifies the IP Security (IPSec) VPN tunnel with a unique, arbitrary name. This name is required.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(4)YA	This command was introduced on Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(8)YJ	This command was enhanced to specify an IPSec VPN tunnel for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(8)YJ	This command was enhanced to specify an IPSec VPN tunnel for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

If the tunnel name is not specified, the authorization request is made on the active tunnel. If there is more than one active tunnel, the command fails with an error requesting that you specify the tunnel name.

When making a VPN connection, individual users might also be required to provide authorization information, such as a username or password. When the remote end requires this information, the router displays a message on the console of the router instructing the user to enter the **crypto ipsec client ezvpn xauth** command. The user then uses command-line interface (CLI) to enter this command and to provide the information requested by the prompts that follow after the command has been entered.

Note If the user does not respond to the authentication notification, the message is repeated every 10 seconds.

Examples

The following example shows an example of the user being prompted to enter the **crypto ipsec client ezvpn xauth** command. The user then enters the requested information and continues.

```
Router#
20:27:39: EZVPN: Pending XAuth Request, Please enter the following command:
20:27:39: EZVPN: crypto ipsec client ezvpn xauth

Router> crypto ipsec client ezvpn xauth
Enter Username and Password: userid
Password: ************
```

Related Commands

Command	Description
crypto ipsec client ezvpn (interface)	Assigns a Cisco Easy VPN Remote configuration to an interface.

crypto ipsec default transform-set

To enable default IP Security (IPsec) transform sets, use the **crypto ipsec default transform-set** command in global configuration mode. To disable the default IPsec transform sets, use the **no** form of this command.

crypto ipsec default transform-set

no crypto ipsec default transform-set

Syntax Description

This command has no arguments or keywords.

Command Default

The default IPsec transform sets are enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

A default transform set will be used by any crypto map or ipsec profile where no other transform set has been configured if the following is true:

- The default transform sets have not been disabled with the **no crypto ipsec default transform-set** command.
- The crypto engine in use supports the encryption algorithm.

Each default transform set defines both an Encapsulation Security Protocol (ESP) encryption transform type and an ESP authentication transform type as shown in Table 22.

Table 22 Default Transform Sets and Parameters

Default Transform Name	ESP Encryption Transform and Description	ESP Authentication Transform and Description
#$!default_transform_set_0	esp-3des (ESP with the 168-bit Triple Data Encryption Standard [3DES or Triple DES] encryption algorithm)	esp-sha-hmac (ESP with the Secure Hash Algorithm [SHA-1, HMAC variant] authentication algorithm)
#$!default_transform_set_1	esp-aes (ESP with the 128-bit Advanced Encryption Standard [AES] encryption algorithm)	esp-sha-hmac

Examples

The following example displays output from the **show crypto ipsec default transform-set** command when the default transform sets are enabled, the default setting.

```
Router# show crypto ipsec default transform-set

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
```

The following example displays output from the **show crypto ipsec default transform-set** command when the default transform sets have been disabled with the **no crypto ipsec default transform-set** command.

```
Router(config)# no crypto ipsec default transform-set
Router(config)# exit
Router#
Router# show crypto ipsec default transform-set
! There is no output.
Router#
```

The following is example system log message that is generated whenever IPsec security associations (SAs) have negotiated with a default transform set.

```
%CRYPTO-5-IPSEC_DEFAULT_TRANSFORM: Using Default IPSec transform-set
```

Related Commands

Command	Description
show crypto isakmp default policy	Displays the default IKE policies currently in use.

crypto ipsec df-bit (global)

To set the DF bit for the encapsulating header in tunnel mode to all interfaces, use the **crypto ipsec df-bit** command in global configuration mode.

crypto ipsec df-bit [**clear** | **set** | **copy**]

Syntax Description

clear	Outer IP header will have the DF bit cleared, and the router may fragment the packet to add the IP Security (IPSec) encapsulation.
set	Outer IP header will have the DF bit set; however, the router may fragment the packet if the original packet had the DF bit cleared.
copy	The router will look in the original packet for the outer DF bit setting. The **copy** keyword is the default setting.

Defaults

The default is **copy**.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

Use the **crypto ipsec df-bit** command in global configuration mode to configure your router to specify the DF bit in an encapsulated header.

You may want use the **clear** setting for the DF bit when encapsulating tunnel mode IPSec traffic so you can send packets larger than the available maximum transmission unit (MTU) size or if you do not know what the available MTU size is.

If this command is enabled without a specified setting, the router will use the **copy** setting as the default.

Examples

The following example shows how to clear the DF bit on all interfaces:

```
crypto ipsec df-bit clear
```

crypto ipsec df-bit (interface)

To set the DF bit for the encapsulating header in tunnel mode to a specific interface, use the **crypto ipsec df-bit** command in interface configuration mode.

crypto ipsec df-bit [**clear** | **set** | **copy**]

Syntax Description

clear	Outer IP header has the DF bit cleared, and the router may fragment the packet to add the IP Security (IPSec) encapsulation.
set	Outer IP header has the DF bit set; however, the router may fragment the packet if the original packet had the DF bit cleared.
copy	The router looks in the original packet for the outer DF bit setting.

Defaults

The default setting is the same as the **crypto ipsec df-bit** command setting in global configuration mode.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

Use the **crypto ipsec df-bit** command in interface configuration mode to configure your router to specify the DF bit in an encapsulated header. This command overrides any existing DF bit global settings.

You may want use the **clear** setting for the DF bit when encapsulating tunnel mode IPSec traffic so you can send packets larger than the available maximum transmission unit (MTU) size or if you do not know what the available MTU size is.

If this command is enabled without a specified setting, the router uses the **crypto ipsec df-bit** command setting in global configuration mode.

Examples

In following example, the router is configured to globally clear the setting for the DF bit and copy the DF bit on the interface named Ethernet0. Thus, all interfaces *except* Ethernet0 allows the router to send packets larger than the available MTU size; Ethernet0 allows the router to fragment the packet.

```
crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp key Delaware address 192.168.10.66
crypto isakmp key Key-What-Key address 192.168.11.19
!
!
crypto ipsec transform-set BearMama ah-md5-hmac esp-des

crypto ipsec df-bit clear
!
!
```

```
crypto map armadillo 1 ipsec-isakmp
set peer 192.168.10.66
set transform-set BearMama
match address 101
!
crypto map basilisk 1 ipsec-isakmp
set peer 192.168.11.19
set transform-set BearMama
match address 102

!
!
interface Ethernet0
 ip address 192.168.10.38 255.255.255.0
 ip broadcast-address 0.0.0.0
 media-type 10BaseT
 crypto map armadillo
 crypto ipsec df-bit copy
!
interface Ethernet1
 ip address 192.168.11.75 255.255.255.0
 ip broadcast-address 0.0.0.0
 media-type 10BaseT
 crypto map basilisk
!
interface Serial0
 no ip address
 ip broadcast-address 0.0.0.0
 no ip route-cache
 no ip mroute-cache
```

crypto ipsec fragmentation (global)

To enable prefragmentation for IP Security (IPSec) Virtual Private Networks (VPNs) on a global basis, use the **crypto ipsec fragmentation** command in global configuration mode. To disable a manually configured command, use the **no** form of this command.

crypto ipsec fragmentation {**before-encryption** | **after-encryption**}

no crypto ipsec fragmentation {**before-encryption** | **after-encryption**}

Syntax Description

before-encryption	Enables prefragmentation for IPSec VPNs. The default is that prefragmentation is enabled.
after-encryption	Disables prefragmentation for IPSec VPNs.

Command Default

If you do not enter this command, prefragmentation is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **before-encryption** keyword to enable prefragmentation for IPSec VPNs; use the **after-encryption** keyword to disable prefragmentation for IPSec VPNs. This command allows an encrypting router to predetermine the encapsulated packet size from information available in transform sets, which are configured as part of the IPSec security association (SA). If it is predetermined that the packet will exceed the maximum transmission unit (MTU) of the output interface, the packet is fragmented before encryption.

Note This command does not show up in the a running configuration if the default global command is enabled. It shows in the running configuration only when you explicitly enable the command on an interface.

Examples

The following example shows how to globally enable prefragmentation for IPSec VPNs:

```
crypto ipsec fragmentation before-encryption
```

crypto ipsec fragmentation (interface)

To enable prefragmentation for IP Security (IPSec) Virtual Private Networks (VPNs) on an interface, use the **crypto ipsec fragmentation** command in interface configuration mode. To disable a manually configured command, use the **no** form of this command.

crypto ipsec fragmentation {**before-encryption** | **after-encryption**}

no crypto ipsec fragmentation {**before-encryption** | **after-encryption**}

Syntax Description

before-encryption	Enables prefragmentation for IPSec VPNs.
after-encryption	Disables prefragmentation for IPSec VPNs.

Defaults

If no other prefragmentation for IPSec VPNs commands are in the configuration, the router will revert to the default global configuration.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **before-encryption** keyword to enable prefragmentation for IPSec VPNs per interface; use the **after-encryption** keyword to disable prefragmentation for IPSec VPNs. This command allows an encrypting router to predetermine the encapsulated packet size from information available in transform sets, which are configured as part of the IPSec security association (SA). If it is predetermined that the packet will exceed the maximum transmission unit (MTU) of output interface, the packet is fragmented before encryption.

Examples

The following example shows how to enable prefragmentation for IPSec VPNs on an interface and then how to display the output of the show running configuration command:

Note This command shows in the running configuration only when you explicitly enable it on the interface.

```
Router(config-if)# crypto ipsec fragmentation before-encryption
Router(config-if)# exit
```

```
Router# show running-config

crypto isakmp policy 10
 authentication pre-share
crypto isakmp key abcd123 address 209.165.202.130
!
crypto ipsec transform-set fooprime esp-3des esp-sha-hmac
!
crypto map bar 10 ipsec-isakmp
 set peer 209.165.202.130
 set transform-set fooprime
 match address 102
```

crypto ipsec ipv4-deny

To configure deny address ranges at the global (IPSec VPN SPA) level, use the **crypto ipsec ipv4 deny-policy** command in global configuration mode.

crypto ipsec ipv4-deny {**jump | clear | drop**}

Syntax Description

jump	Causes the search to jump to the beginning of the ACL associated with the next sequence in the crypto map and continues the search when a deny address is hit.
clear	Allows traffic to pass through in the clear (unencrypted) state when a deny address is hit.
drop	Causes traffic to be dropped when a deny address is hit.

Command Modes

The default behavior is **jump**.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to prevent repeated address ranges from being programmed in the hardware, resulting in more efficient TCAM space utilization.

Specifying a deny address range in an ACL results in “jump” behavior. When a denied address range is hit, it forces the search to “jump” to the beginning of the ACL associated with the next sequence in a crypto map and continue the search.

The **clear** keyword allows a deny address range to be programmed in hardware. The deny addresses are then filtered out for encryption and decryption. If the voice private network (VPN) mode is crypto-connect, when a deny address is hit, the search is stopped and traffic is allowed to pass in the clear (unencrypted) state.

If the VPN mode is VRF mode, the deny address matching traffic is dropped.

If you want to pass clear traffic on an address, you must insert a deny address range for each sequence in a crypto map.

Each permit list of addresses inherits all the deny address ranges specified in the ACL. A deny address range causes the software to do a subtraction of the deny address range from a permit list, and creates multiple permit address ranges that need to be programmed in hardware. This behavior can cause repeated address ranges to be programmed in the hardware for a single deny address range, resulting in multiple permit address ranges in a single ACL.

If you apply the specified keyword **(jump**, **clear**, or **drop**) when crypto maps are already configured on the IPSec VPN SPA, all existing IPSec sessions are temporarily removed and restarted, which impacts traffic on your network.

The number of deny entries that can be specified in an ACL are dependent on the keyword specified:

- **jump**—Supports up to 8 deny entries in an ACL.
- **clear**—Supports up to 1000 deny entries in an ACL.
- **drop**—Supports up to 1000 deny entries in an ACL.

Examples

The following example shows a configuration using the deny-policy **clear** option. In this example, when a deny address is hit, the search will stop and traffic will be allowed to pass in the clear (unencrypted) state:

```
Router(config)# crypto ipsec ipv4-deny clear
```

Related Commands

Command	Description
access-list	Defines a standard or extended IP access list.

crypto ipsec nat-transparency

To enable security parameter index (SPI) matching or User Datagram Protocol (UDP) encapsulation between two Virtual Private Network (VPN) devices, use the **crypto ipsec nat-transparency** command on both devices in global configuration mode. To disable both SPI matching and UDP encapsulation, use the **no** form of this command with each keyword.

crypto ipsec nat-transparency {**spi-matching** | **udp-encaps**}

no crypto ipsec nat-transparency {**spi-matching** | **udp-encaps**}

Syntax Description

spi-matching	Enables SPI matching on both endpoints.
udp-encaps	Enables UDP encapsulation on both endpoints.

Defaults

When this command is entered, UDP encapsulation is enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(15)T	The command syntax was modified to add the **spi-matching** keyword.

Usage Guidelines

You can use this command to resolve issues that arise when Network Address Translation (NAT) is configured in an IP Security (IPsec)-aware network. This command has two mutually exclusive options:

- The default option is UDP encapsulation of the IPsec protocols.
- The alternative is to match the inbound SPI to the outbound SPI.

When you enter the **crypto ipsec nat-transparency** command, UDP encapsulation is configured unless you either specifically disable it or configure SPI matching. You can disable both options, but doing so might cause problems if the device you are configuring uses NAT and is part of a VPN.

To disable SPI matching, configure UDP encapsulation or use the **no** form of this command with the keyword **spi-matching**. To disable UDP encapsulation, configure SPI matching or use the **no** form of this command with the keyword **udp-encaps**. To disable both SPI matching and UDP encapsulation, first disable UDP encapsulation, and then disable SPI matching. If you disable both options, the **show running-config** command displays: **no crypto ipsec nat-transparency udp-encaps.**

Examples

The following example enables SPI matching on the endpoint routers:

```
crypto ipsec nat-transparency spi-matching
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.
show crypto isakmp sa detail nat	Displays NAT translations of source and destination addresses.

crypto ipsec optional

To enable IP Security (IPSec) passive mode, use the **crypto ipsec optional** command in global configuration mode. To disable IPSec passive mode, use the **no** form of this command.

crypto ipsec optional

no crypto ipsec optional

Syntax Description

This command has no arguments or keywords.

Defaults

IPSec passive mode is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use the **crypto ipsec optional** command to implement an intermediate mode (IPSec passive mode) that allows a router to accept unencrypted and encrypted data. IPSec passive mode is valuable for users who wish to migrate existing networks to IPSec because all routers will continue to interact with routers that encrypt data (that is, that have been upgraded with IPSec) and also with routers that have yet to be upgraded.

After this feature is disabled, all active connections that are sending unencrypted packets are cleared, and a message that reminds the user to enter the **write memory** command is sent.

Note Because a router in IPSec passive mode is insecure, ensure that no routers are accidentally left in this mode after upgrading a network.

Examples

The following example shows how to enable IPSec passive mode:

```
crypto map xauthmap 10 ipsec-isakmp
 set peer 209.165.202.145
 set transform-set xauthtransform
 match address 192
!
crypto ipsec optional
!
interface Ethernet1/0
 ip address 209.165.202.147 255.255.255.224
 crypto map xauthmap
!
access-list 192 permit ip host 209.165.202.147 host 209.165.202.145
```

crypto ipsec optional retry

To adjust the amount of time that a packet can be routed in the clear (unencrypted), use the **crypto ipsec optional retry** command in global configuration mode. To return to the default setting (5 minutes), use the **no** form of this command.

crypto ipsec optional retry *seconds*

no crypto ipsec optional retry *seconds*

Syntax Description

seconds	Time a connection can exist before another attempt is made to establish an encrypted IP Security (IPSec) session. The default value is 5 minutes.

Defaults

5 minutes

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

You must enable the **crypto ipsec optional** command, which enables IPSec passive mode, before you can use this command.

Examples

The following example shows how to enable IPSec passive mode:

```
crypto map xauthmap 10 ipsec-isakmp
 set peer 209.165.202.145
 set transform-set xauthtransform
 match address 192
!
crypto ipsec optional
crypto ipsec optional retry 60
!
interface Ethernet1/0
 ip address 209.165.202.147 255.255.255.224
 crypto map xauthmap
!
access-list 192 permit ip host 209.165.202.147 host 209.165.202.145
```

Related Commands

Command	Description
crypto ipsec optional	Enables IPSec passive mode.

crypto ipsec profile

To define the IP Security (IPsec) parameters that are to be used for IPsec encryption between two IPsec routers and to enter IPsec profile configuration mode, use the **crypto ipsec profile** command in global configuration mode. To delete an IPsec profile, use the **no** form of this command.

crypto ipsec profile *name*

no crypto ipsec profile *name*

Syntax Description

name	Profile name.

Command Default

An IPsec profile is not defined.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.4(4)T	Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

An IPsec profile abstracts the IPsec policy settings into a single profile that can be used in other parts of the Cisco IOS configuration.

The IPsec profile shares most of the same commands with the crypto map configuration, but only a subset of the commands are valid in an IPsec profile. Only commands that pertain to an IPsec policy can be issued under an IPsec profile; you cannot specify the IPsec peer address or the access control list (ACL) to match the packets that are to be encrypted.

After this command has been enabled, the following commands can be configured under an IPsec profile:

- **default**—Lists the commands that can be configured under the **crypto ipsec profile** command.
- **description**—Describes the crypto map statement policy.
- **dialer**—Specifies dialer-related commands.
- **redundancy**—Specifies a redundancy group name.
- **set-identity**—Specifies identity restrictions.
- **set isakmp-profile**—Specifies an ISAKMP profile.
- **set pfs**—Specifies perfect forward secrecy (PFS) settings.
- **set security-association**—Defines security association parameters.
- **set-transform-set**—Specifies a list of transform sets in order of priority.

After enabling this command, the only parameter that *must* be defined under the profile is the transform set via the **set transform-set** command.

For more information on transform sets, refer to the section "Defining Transform Sets" in the chapter "Configuring IPSec Network Security" in the *Cisco IOS Security Configuration Guide*.

Examples

The following example shows how to configure a crypto map that uses an IPsec profile:

```
crypto ipsec transform-set cat-transforms esp-des esp-sha-hmac
 mode transport
!
crypto ipsec profile cat-profile
 set transform-set cat-transforms
 set pfs group2
!
interface Tunnel1
 ip address 192.168.1.1 255.255.255.252
 tunnel source FastEthernet2/0
 tunnel destination 10.13.7.67
 tunnel protection ipsec profile cat-profile
```

Related Commands

Command	Description
crypto ipsec transform-set	Defines a transform set.
set pfs	Specifies that IPsec should ask for PFS when requesting new security associations for a crypto map entry.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
tunnel protection	Associates a tunnel interface with an IPsec profile.

crypto ipsec security-association idle-time

To configure the IP Security (IPSec) security association (SA) idle timer, use the **crypto ipsec security-association idle-time** command in global configuration mode or crypto map configuration mode. To inactivate the IPSec SA idle timer, use the **no** form of this command.

crypto ipsec security-association idle-time *seconds*

no crypto ipsec security-association idle-time

Syntax Description

seconds	Time, in seconds, that the idle timer allows an inactive peer to maintain an SA. The range is 60 to 86400 seconds.

Defaults

IPSec SA idle timers are disabled.

Command Modes

Global configuration
Crypto map configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use the **crypto ipsec security-association idle-time** command to configure the IPSec SA idle timer. This timer controls the amount of time that an SA will be maintained for an idle peer.

Use the **crypto ipsec security-association lifetime** command to configure global lifetimes for IPSec SAs. There are two lifetimes: a timed lifetime and a traffic-volume lifetime. A security association expires after the first of these lifetimes is reached.

The IPSec SA idle timers are different from the global lifetimes for IPSec SAs. The expiration of the global lifetimes is independent of peer activity. The IPSec SA idle timer allows SAs associated with inactive peers to be deleted before the global lifetime has expired.

If the IPSec SA idle timers are not configured with the **crypto ipsec security-association idle-time** command, only the global lifetimes for IPSec SAs are applied. SAs are maintained until the global timers expire, regardless of peer activity.

Note If the last IPSec SA to a given peer is deleted due to idle timer expiration, the Internet Key Exchange (IKE) SA to that peer will also be deleted.

Release 12.2(33)SRA or later releases
Release 12.2(33)SXH or later releases

In a system using the IPSec VPN SPA with these software releases, the configured value for the *seconds* argument is rounded up to the next multiple of 600 seconds (ten minutes), and the rounded value becomes the polling interval for SA idle detection. Because the SA idle condition must be observed in two successive pollings, the period of inactivity may last up to twice the polling period before the SAs are deleted.

Examples

The following example configures the IPSec SA idle timer to drop SAs for inactive peers after at least 750 seconds:

```
Router# configure terminal
Router(config)# crypto ipsec security-association idle-time 750
```

With Cisco IOS Release 12.2(15)T or later releases, the SA will be deleted after an inactivity period of 750 seconds.

With Cisco IOS Release 12.2(33)SRA or 12.2(33)SXH or later releases, the configured value of 750 seconds will be rounded up to 1200 seconds (the next multiple of 600), which becomes the idle polling interval. The SA will be deleted after two successive idle pollings, resulting in an inactivity period of between 1200 and 2400 seconds before deletion.

Related Commands

Command	Description
clear crypto sa	Deletes IPSec SAs.
crypto ipsec security-association lifetime	Changes global lifetime values used when negotiating IPSec SAs.

crypto ipsec security-association lifetime

To change global lifetime values used when negotiating IPsec security associations, use the **crypto ipsec security-association lifetime** command in global configuration mode. To reset a lifetime to the default value, use the **no** form of this command.

crypto ipsec security-association lifetime {**seconds** *seconds* | **kilobytes** *kilobytes* | **kilobytes disable**}

no crypto ipsec security-association lifetime {**seconds** | **kilobytes** | **kilobytes disable**}

Syntax Description

seconds *seconds*	Specifies the number of seconds a security association will live before expiring. The default is 3600 seconds (one hour).
kilobytes *kilobytes*	Specifies the volume of traffic (in kilobytes) that can pass between IPsec peers using a given security association before that security association expires. The default is 4,608,000 kilobytes.
kilobytes disable	Disables the Internet Key Exchange (IKE) rekey based on volume only on the router on which it is configured. • If the **no** form is used with this keyword, lifetime settings switch back to the default settings.

Defaults

3600 seconds (one hour) and 4,608,000 kilobytes (10 megabits per second for one hour).

Command Modes

Global configuration

Command History

Release	Modification
11.3T	This command was introduced.
12.2(13)T	The security association negotiation changed. Prior to Cisco IOS Release 12.2(13)T, the new security association was negotiated either 30 seconds before the **seconds** lifetime expired or when the volume of traffic through the tunnel reached 256 kilobytes less than the **kilobytes** lifetime. Effective with Cisco IOS Release 12.2(13)T, the negotiation is either 30 seconds before the **seconds** lifetime expires or when the volume of traffic through the tunnel reaches 90 percent of the **kilobytes** lifetime.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SXI	The **disable** keyword was added. **Note** This keyword addition is for only Cisco IOS Release 12.2(33)SXI.
15.0(1)M	The **disable** keyword was added.

Usage Guidelines

IPsec security associations use shared secret keys. These keys and their security associations time out together.

Assuming that the particular crypto map entry does not have lifetime values configured, when the router requests new security associations during security association negotiation, it will specify its global lifetime value in the request to the peer; it will use this value as the lifetime of the new security associations. When the router receives a negotiation request from the peer, it will use the smaller of the lifetime value proposed by the peer or the locally configured lifetime value as the lifetime of the new security associations.

There are two lifetimes: a "timed" lifetime and a "traffic-volume" lifetime. The security association expires after the first of these lifetimes is reached.

If you change a global lifetime, the change is only applied when the crypto map entry does not have a lifetime value specified. The change will not be applied to existing security associations, but will be used in subsequent negotiations to establish new security associations. If you want the new settings to take effect sooner, you can clear all or part of the security association database by using the **clear crypto sa** command. Refer to the **clear crypto sa** command for more details.

To change the global timed lifetime, use the **crypto ipsec security-association lifetime seconds** form of the command. The timed lifetime causes the security association to time out after the specified number of seconds have passed.

To change the global traffic-volume lifetime, use the **crypto ipsec security-association lifetime kilobytes** form of the command. The traffic-volume lifetime causes the security association to time out after the specified amount of traffic (in kilobytes) has been protected by the key of the security association.

Shorter lifetimes can make it harder to mount a successful key recovery attack, since the attacker has less data encrypted under the same key to work with. However, shorter lifetimes require more CPU processing time for establishing new security associations.

The lifetime values are ignored for manually established security associations (security associations installed using an **ipsec-manual** crypto map entry).

How The Lifetimes Work

The security association (and corresponding keys) will expire according to whichever occurs sooner, either after the number of seconds has passed (specified by the **seconds** keyword) or after the amount of traffic in kilobytes has passed (specified by the **kilobytes** keyword).

A new security association is negotiated *before* the lifetime threshold of the existing security association is reached, to ensure that a new security association is ready for use when the old one expires. The **seconds** lifetime and the **kilobytes** lifetime each have a jitter mechanism to avoid security association rekey collisions. The new security association is negotiated either (30 plus a random number of) seconds before the **seconds** lifetime expires or when the traffic volume reaches (90 minus a random number of) percent of the **kilobytes** lifetime (whichever occurs first).

If no traffic has passed through the tunnel during the entire life of the security association, a new security association is not negotiated when the lifetime expires. Instead, a new security association will be negotiated only when IPsec sees another packet that should be protected.

Disabling the Volume Lifetime

The **crypto ipsec security-association lifetime kilobytes disable** form of the command disables the volume lifetime. Using this command form should result in a significant improvement in performance and reliability, and this option can be used to reduce packet loss in high traffic environments. It can be used to prevent frequent rekeys that are triggered by reaching the volume lifetimes.

Note The volume lifetime can also be disabled using the **set security-association lifetime kilobytes disable** command.

Examples

The following example shortens both lifetimes, because the administrator feels there is a higher risk that the keys could be compromised. The timed lifetime is shortened to 2700 seconds (45 minutes), and the traffic-volume lifetime is shortened to 2,304,000 kilobytes (10 megabits per second for one half hour).

```
crypto ipsec security-association lifetime seconds 2700
crypto ipsec security-association lifetime kilobytes 2304000
```

The following example shows that the **kilobytes disable** keyword has been used to disable the volume lifetime.

```
crypto ipsec security-association lifetime kilobytes disable
```

Related Commands

Command	Description
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPsec security associations.
show crypto ipsec security-association lifetime	Displays the security-association lifetime value configured for a particular crypto map entry.

crypto ipsec security-association replay disable

To disable anti-replay checking globally, use the **crypto ipsec security-association replay disable** command in global configuration mode. To reset the configuration to enable anti-replay checking, use the **no** form of this command.

crypto ipsec security-association replay disable

no crypto ipsec security-association replay disable

Syntax Description

This command has no arguments or keywords.

Defaults

Anti-replay checking is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF6	This command was integrated into Cisco IOS Release 12.2(18)SXF6.

Examples

The following example shows that anti-replay checking has been disabled globally:

```
crypto map mymap 10
exit
crypto ipsec security-association replay disable
```

Related Commands

Command	Description
crypto ipsec security-association replay window-size	Sets the size of the SA anti-replay window.

crypto ipsec security-association replay window-size

To set the size of the security association (SA) anti-replay window globally, use the **crypto ipsec security-association replay window-size** command in global configuration mode. To reset the window size to the default of 64, use the **no** form of this command.

crypto ipsec security-association replay window-size [*N*]

no crypto ipsec security-association replay window-size

Syntax Description

N	(Optional) Size of the window. Values can be 64, 128, 256, 512, or 1024. This value becomes the default value. **Note** The window size is significant only if anti-replay checking is enabled.

Defaults

If a window size is not entered, the default is 64.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF6	This command was integrated into Cisco IOS Release 12.2(18)SXF6.

Examples

The following example shows that the size of the SA anti-replay window has been set globally to 128:

```
crypto map mymap 20
exit
crypto ipsec security-association replay window-size 128
```

Related Commands

Command	Description
crypto ipsec security-association replay disable	Disables anti-replay checking.

crypto ipsec server send-update

To send auto-update notifications any time after an Easy VPN connection is "up," use the **crypto ipsec server send-update** command in privileged EXEC mode.

crypto ipsec server send-update {*group-name*}

no crypto ipsec server send-update {*group-name*}

Syntax Description

group-name	Name of group to which to send auto-update notifications.

Command Default

Auto-update notifications are not sent.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(2T)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

This command is configured on a server. By configuring the command, the auto update notification is sent manually after the tunnel is "up."

Examples

The following example shows that automatic update notifications are to be sent to GroupA:

```
crypto ipsec server send-update GroupA
```

crypto ipsec transform-set

To define a transform set—an acceptable combination of security protocols and algorithms—use the **crypto ipsec transform-set** command in global configuration mode. To delete a transform set, use the **no** form of this command.

crypto ipsec transform-set *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]

no crypto ipsec transform-set *transform-set-name*

Syntax Description

transform-set-name	Name of the transform set to create (or modify).
transform1 *transform2* *transform3* *transform4*	Type of transform set. You may specify up to four "transforms": one Authentication Header (AH), one Encapsulating Security Payload (ESP) encryption, one ESP authentication, and one compression. These transforms define the IP Security (IPSec) security protocols and algorithms. Accepted transform values are described in Table 23.

Defaults

No default behavior or values

Command Modes

Global configuration

This command invokes the crypto transform configuration mode.

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(13)T	The following transform set options were added: **esp-aes**, **esp-aes 192**, and **esp-aes 256**.
12.3(7)T	The **esp-seal** transform set option was added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(2)T	This command was modified in Cisco IOS Release 15.1(2)T. The **esp-gcm** and **esp-gmac** transforms were added.

Usage Guidelines

A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPSec-protected traffic. During the IPSec security association (SA) negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

You can configure multiple transform sets, and then specify one or more of these transform sets in a crypto map entry. The transform set defined in the crypto map entry is used in the IPSec SA negotiation to protect the data flows specified by the access list of that crypto map entry. During the negotiation, the peers search for a transform set that is the same at both peers. When such a transform set is found, it is selected and will be applied to the protected traffic as part of the IPSec SAs of both peers.

When Internet Key Exchange (IKE) is not used to establish SAs, a single transform set must be used. The transform set is not negotiated.

Before a transform set can be included in a crypto map entry, it must be defined using this command.

A transform set specifies one or two IPSec security protocols (either AH, ESP, or both) and specifies which algorithms to use with the selected security protocol. The AH and ESP IPSec security protocols are described in the section "IPSec Protocols: AH and ESP."

To define a transform set, you specify one to four "transforms"—each transform represents an IPSec security protocol (AH or ESP) plus the algorithm you want to use. When the particular transform set is used during negotiations for IPSec SAs, the entire transform set (the combination of protocols, algorithms, and other settings) must match a transform set at the remote peer.

In a transform set you can specify the AH protocol, the ESP protocol, or both. If you specify an ESP protocol in a transform set, you can specify just an ESP encryption transform set or both an ESP encryption transform set and an ESP authentication transform set.

Table 23 lists the acceptable transform set combination selections for the AH and ESP protocols.

Table 23 Allowed Transform Combinations

Transform Type	Transform	Description
AH Transform (*Pick only one.*)	**ah-md5-hmac**	AH with the MD5 (Message Digest 5) (a Hash-based Message Authentication Code [HMAC] variant) authentication algorithm.
	ah-sha-hmac	AH with the SHA (Secure Hash Algorithm) (an HMAC variant) authentication algorithm.

Table 23 Allowed Transform Combinations (continued)

Transform Type	Transform	Description
ESP Encryption Transform (*Pick only one.*)	**esp-aes**	ESP with the 128-bit Advanced Encryption Standard (AES) encryption algorithim.
	esp-gcm **esp-gmac**	The **esp-gcm** and **esp-gmac** transforms are ESPs with either a 128 or 256 bit encryption algorithm. The default for either of these transforms is 128 bits. **Note** Both the **esp-gcm** and **esp-gmac** transforms cannot be configured together with any other ESP transform within the same crypto IPsec transform set using the **crypto ipsec transform-set** command.
	esp-aes 192	ESP with the 192-bit AES encryption algorithim.
	esp-aes 256	ESP with the 256-bit AES encryption algorithim.
	esp-des	ESP with the 56-bit Data Encryption Standard (DES) encryption algorithm.
	esp-3des	ESP with the 168-bit DES encryption algorithm (3DES or Triple DES).
	esp-null	Null encryption algorithm.
	esp-seal	ESP with the 160-bit SEAL encryption algorithm.
ESP Authentication Transform (*Pick only one.*)	**esp-md5-hmac**	ESP with the MD5 (HMAC variant) authentication algorithm.
	esp-sha-hmac	ESP with the SHA (HMAC variant) authentication algorithm.
IP Compression Transform	**comp-lzs**	IP compression with the Lempel-Ziv-Stac (LZS) algorithm

Examples of acceptable transform set combinations are as follows:

- **ah-md5-hmac**
- **esp-gcm 256**
- **esp-des**
- **esp-3des** and **esp-md5-hmac**
- **ah-sha-hmac** and **esp-des** and **esp-sha-hmac**

- **comp-lzs** and **esp-sha-hmac** and **esp-aes** (In general, the **comp-lzs** transform set can be included with any other legal combination that does not already include the **comp-lzs** transform.)
- esp-seal and esp-md5-hmac

The parser will prevent you from entering invalid combinations; for example, after you specify an AH transform set, it will not allow you to specify another AH transform set for the current transform set.

IPSec Protocols: AH and ESP

Both the AH and ESP protocols implement security services for IPSec.

AH provides data authentication and antireplay services.

ESP provides packet encryption and optional data authentication and antireplay services.

ESP encapsulates the protected data—either a full IP datagram (or only the payload)—with an ESP header and an ESP trailer. AH is embedded in the protected data; it inserts an AH header immediately after the outer IP header and before the inner IP datagram or payload. Traffic that originates and terminates at the IPSec peers can be sent in either tunnel or transport mode; all other traffic is sent in tunnel mode. Tunnel mode encapsulates and protects a full IP datagram, while transport mode encapsulates or protects the payload of an IP datagram. For more information about modes, see the **mode** (IPSec) command description.

The esp-seal Transform

There are three limitations on the use of the **esp-seal** transform set:

- The **esp-seal** transform set can be used only if no crypto accelerators are present. This limitation is present because no current crypto accelerators implement the SEAL encryption transform set, and if a crypto accelerator is present, it will handle all IPSec connections that are negotiated with IKE. If a crypto accelerator is present, the Cisco IOS software will allow the transform set to be configured, but it will warn that it will not be used as long as the crypto accelerator is enabled.
- The **esp-seal** transform set can be used only in conjunction with an authentication transform set, namely one of these: **esp-md5-hmac**, **esp-sha-hmac**, **ah-md5-hmac**, or **ah-sha-hmac**. This limitation is present because SEAL encryption is especially weak when it comes to protecting against modifications of the encrypted packet. Therefore, to prevent such a weakness, an authentication transform set is required. (Authentication transform sets are designed to foil such attacks.) If you attempt to configure an IPSec transform set using SEAL but without an authentication transform set, an error is generated, and the transform set is rejected.
- The **esp-seal** transform set cannot be used with a manually keyed crypto map. This limitation is present because such a configuration would reuse the same keystream for each reboot, which would compromise security. Because of the security issue, such a configuration is prohibited. If you attempt to configure a manually keyed crypto map with a SEAL-based transform set, an error is generated, and the transform set is rejected.

Selecting Appropriate Transform Sets

The following tips may help you select transform sets that are appropriate for your situation:

- If you want to provide data confidentiality, include an ESP encryption transform set.
- If you want to ensure data authentication for the outer IP header as well as the data, include an AH transform set. (Some consider the benefits of outer IP header data integrity to be debatable.)
- If you use an ESP encryption transform set, also consider including an ESP authentication transform set or an AH transform set to provide authentication services for the transform set.

- If you want data authentication (either using ESP or AH), you can choose from the MD5 or SHA (HMAC keyed hash variants) authentication algorithms. The SHA algorithm is generally considered stronger than MD5 but is slower.
- Note that some transform sets might not be supported by the IPSec peer.

Note If a user enters an IPSec transform set that the hardware does not support, a warning message will be displayed immediately after the **crypto ipsec transform-set** command is entered.

- In cases where you need to specify an encryption transform set but do not actually encrypt packets, you can use the **esp-null** transform.

Suggested transform set combinations follow:

- **esp-3des** and **esp-sha-hmac**
- **esp-aes** and **esp-md5-hmac**

The Crypto Transform Configuration Mode

After you issue the **crypto ipsec transform-set** command, you are put into the crypto transform configuration mode. While in this mode, you can change the mode to tunnel or transport. (These are optional changes.) After you have made these changes, type **exit** to return to global configuration mode. For more information about these optional changes, see the **match address** (IPSec) and **mode** (IPSec) command descriptions.

Changing Existing Transform Sets

If one or more transform sets are specified in the **crypto ipsec transform-set** command for an existing transform set, the specified transform sets will replace the existing transform sets for that transform set.

If you change a transform set definition, the change is only applied to crypto map entries that reference the transform set. The change will not be applied to existing SAs but will be used in subsequent negotiations to establish new SAs. If you want the new settings to take effect sooner, you can clear all or part of the SA database by using the **clear crypto sa** command.

Examples

The following example defines two transform sets. The first transform set will be used with an IPSec peer that supports the newer ESP and AH protocols. The second transform set will be used with an IPSec peer that supports only the older transforms.

```
Router (config)# crypto ipsec transform-set newer esp-3des esp-sha-hmac
Router (config)# crypto ipsec transform-set older ah-rfc-1828 esp-rfc1829
```

The following example is a sample warning message that is displayed when a user enters an IPSec transform set that the hardware does not support:

```
Router (config)# crypto ipsec transform transform-1 esp-aes 256 esp-md5
WARNING:encryption hardware does not support transform
esp-aes 256 within IPSec transform transform-1
```

The following output example shows that SEAL encryption has been correctly configured with an authentication transform set:

```
Router (config)# crypto ipsec transform-set seal esp-seal esp-sha-hmac
```

The following example is a warning message that is displayed when SEAL encryption has been configured with a crypto accelerator present:

```
Router (config)# show running-config
```

```
crypto ipsec transform-set seal esp-seal esp-sha-hmac
! Disabled because transform not supported by encryption hardware
```

The following example is an error message that is displayed when SEAL encryption has been configured without an authentication transform set:

```
Router (config)# crypto ipsec transform seal esp-seal
ERROR: Transform requires either ESP or AH authentication.
```

The following example is an error message that is displayed when SEAL encryption has been configured within a manually keyed crypto map:

```
Router (config)# crypto map green 10 ipsec-manual
%Note: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router (config-crypto-map)# set transform seal
ERROR: transform seal illegal for a manual crypto map.
```

Related Commands

Command	Description
clear crypto sa	Deletes IPSec security associations.
crypto ipsec transform-set	Defines a transform set—an acceptable combination of security protocols and algorithms.
match address	Specifies an extended access list for a crypto map entry.
mode (IPSec)	Changes the mode for a transform set.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto ipsec transform-set	Displays the configured transform sets.

crypto isakmp aggressive-mode disable

To block all Internet Security Association and Key Management Protocol (ISAKMP) aggressive mode requests to and from a device, use the **crypto isakmp aggressive-mode disable** command in global configuration mode. To disable the blocking, use the **no** form of this command.

crypto isakmp aggressive-mode disable

no crypto isakmp aggressive-mode disable

Syntax Description

This command has no arguments or keywords.

Defaults

If this command is not configured, Cisco IOS software will attempt to process all incoming ISAKMP aggressive mode security association (SA) connections. In addition, if the device has been configured with the **crypto isakmp peer address** and the **set aggressive-mode password** or **set aggressive-mode client-endpoint** commands, the device will initiate aggressive mode if this command is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced on all Cisco IOS platforms that support IP Security (IPSec).

Usage Guidelines

If you configure this command, all aggressive mode requests to the device and all aggressive mode requests made by the device are blocked, regardless of the ISAKMP authentication type (preshared keys or Rivest, Shamir, and Adelman [RSA] signatures).

If a request is made by or to the device for aggressive mode, the following syslog notification is sent:

```
Unable to initiate or respond to Aggressive Mode while disabled
```

Note This command will prevent Easy Virtual Private Network (Easy VPN) clients from connecting if they are using preshared keys because Easy VPN clients (hardware and software) use aggressive mode.

Examples

The following example shows that all aggressive mode requests to and from a device are blocked:

```
Router (config)# crypto isakmp aggressive-mode disable
```

crypto isakmp client configuration address-pool local

To configure the IP address local pool to reference Internet Key Exchange (IKE) on your router, use the **crypto isakmp client configuration address-pool local** command in global configuration mode. To restore the default value, use the **no** form of this command.

crypto isakmp client configuration address-pool local *pool-name*

no crypto isakmp client configuration address-pool local

Syntax Description

pool-name	Specifies the name of a local address pool.

Defaults

IP address local pools do not reference IKE.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XE	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS release 12.0(7)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example references IP address local pools to IKE on your router, with “ire” as the *pool-name*:

```
crypto isakmp client configuration address-pool local ire
```

Related Commands

Command	Description
ip local pool	Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.

crypto isakmp client configuration browser-proxy

To configure browser-proxy parameters for an Easy VPN remote device and to enter ISAKMP browser proxy configuration mode, use the **crypto isakmp client configuration browser-proxy** command in global configuration mode. To disable the browser-proxy parameters, use the **no** form of this command.

crypto isakmp client configuration browser-proxy {*browser-proxy-name*}

no crypto isakmp client configuration browser-proxy {*browser-proxy-name*}

Syntax Description

browser-proxy-name	Name of the browser proxy.

Command Default

Browser-proxy parameters are not set.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

While specifying the proxy server, the proxy IP address and port number are separated with a colon. The proxy exception list is a semicolon-delimited string of IP addresses.

After enabling this command, you may specify the following subcommand:

- **proxy**—Configures proxy parameters for your Easy VPN remote device (see the **proxy** command for more information about this command and the acceptable parameters).

Examples

The following example shows various browser-proxy parameter settings for a browser proxy named "bproxy":

```
crypto isakmp client configuration browser-proxy bproxy
 proxy auto-detect

crypto isakmp client configuration browser-proxy bproxy
 proxy none

crypto isakmp client configuration browser-proxy bproxy
 proxy server 10.1.1.1:2000
 proxy exception-list 10.2.2.*,www.*org
 proxy by-pass-local
```

Related Commands

Command	Description
proxy	Configures proxy parameters for an Easy VPN remote device.

crypto isakmp client configuration group

To specify to which group a policy profile will be defined and to enter crypto ISAKMP group configuration mode, use the **crypto isakmp client configuration group** command in global configuration mode. To remove this command and all associated subcommands from your configuration, use the **no** form of this command.

crypto isakmp client configuration group {*group-name* | **default**}

no crypto isakmp client configuration group

Syntax Description

group-name	Group definition that identifies which policy is enforced for users.
default	Policy that is enforced for all users who do not offer a group name that matches a *group-name* argument. The **default** keyword can only be configured locally.

Defaults

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.3(2)T	The **access-restrict**, **firewall are-u-there**, **group-lock**, **include-local-lan**, and **save-password** commands were added. These commands are added during Mode Configuration. In addition, this command was modified so that output for this command will show that the preshared key is either encrypted or unencrypted.
12.3(4)T	The **backup-gateway**, **max-logins**, **max-users,** and **pfs** commands were added.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(2)T	The **browser-proxy** command was added.
12.4(6)T	The **firewall policy** command was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(9)T	The **crypto aaa attribute list**, **dhcp server,** and **dhcp timeout** commands were added.
12.4(11)T	The **dhcp giaddr** command was added.

Usage Guidelines

Use the **crypto isakmp client configuration group** command to specify group policy information that needs to be defined or changed. You may wish to change the group policy on your router if you decide to connect to the client using a group ID that does not match the *group-name* argument.

After enabling this command, which puts you in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode, you can specify characteristics for the group policy using the following commands:

- **access-restrict**—Ties a particular Virtual Private Network (VPN) group to a specific interface for access to the Cisco IOS gateway and the services it protects.
- **acl**—Configures split tunneling.
- **auto-update client**—Configures auto upgrade.
- **backup-gateway**—Configures a server to "push down" a list of backup gateways to the client. These gateways are tried in order in the case of a failure of the previous gateway. The gateways may be specified using IP addresses or host names.
- **banner**—Specifies a mode configuration banner.
- **browser-proxy**—Applies a browser-proxy map to a group.
- **configuration url**—Specifies on a server the URL an Easy VPN remote device must use to get a configuration in a Mode Configuration Exchange.
- **configuration version**—Specifies on a server the version a Cisco Easy VPN remote device must use to get a particular configuration in a Mode Configuration Exchange.
- **crypto aaa attribute list**—Defines a AAA attribute list of per-user attributes on a local Easy VPN server.
- **dhcp giaddr**—Configures an IP address on the Easy VPN server for the Dynamic Host Configuration Protocol (DHCP) to use. The DHCP server uses the giaddr keyword to determine the scope for the client IP address assignment. If the giaddr keyword is not configured, the Easy VPN server must be configured with a loopback interface to communicate with the DHCP server, and the IP address on the loopback interface determines the scope for the client IP address assignment.
- **dhcp server**—Configures multiple DHCP server entries.
- **dhcp timeout**—Controls the wait time before the next DHCP server on the list is tried.
- **dns**—Specifies the primary and secondary Domain Name Service (DNS) servers for the group.
- **domain**—Specifies group domain membership.
- **firewall are-u-there—**Adds the Firewall-Are-U-There attribute to the server group if your PC is running the Black Ice or Zone Alarm personal firewalls.
- **firewall policy**—Specifies the CPP firewall policy push name for the crypto ISAKMP client configuration group on a local AAA server.
- **group-lock**—Use if preshared key authentication is used with Internet Key Exchange (IKE). Allows you to enter your extended authentication (Xauth) username. The group delimiter is compared against the group identifier sent during IKE aggressive mode.
- **include-local-lan—**Configures the Include-Local-LAN attribute to allow a nonsplit-tunneling connection to access the local subnetwork at the same time as the client.
- **key**—Specifies the IKE preshared key when defining group policy information for Mode Configuration push.
- **max-logins**—Limits the number of simultaneous logins for users in a specific user group.
- **max-users**—Limits the number of connections to a specific server group.
- **netmask**—Subnet mask to be used by the client for local connectivity.

- **pfs**—Configures a server to notify the client of the central-site policy regarding whether PFS is required for any IPsec SA. Because the client device does not have a user interface option to enable or disable PFS negotiation, the server will notify the client device of the central site policy via this parameter. The Diffie-Hellman (D-H) group that is proposed for PFS will be the same that was negotiated in Phase 1 of the IKE negotiation.
- **pool**—Refers to the IP local pool address used to allocate internal IP addresses to clients.
- **save-password**—Saves your Xauth password locally on your PC.
- **split-dns**—Specifies a list of domain names that must be tunneled or resolved to the private network.
- **wins**—Specifies the primary and secondary Windows Internet Naming Service (WINS) servers for the group.

Output for the **crypto isakmp client configuration group** command (using the **key** subcommand) will show that the preshared key is either encrypted or unencrypted. An output example for an unencrypted preshared key would be as follows:

```
crypto isakmp client configuration group key test
```

An output example for a type 6 encrypted preshared key would be as follows:

```
crypto isakmp client configuration group
 key 6 JK_JHZPeJV_XFZTKCQFYAAB
```

Session Monitoring and Limiting for Easy VPN Clients

It is possible to mimic the functionality provided by some RADIUS servers for limiting the number of connections to a specific server group and also for limiting the number of simultaneous logins for users in that group.

To limit the number of connections to a specific server group, use the **max-users** subcommand. To limit the number of simultaneous logins for users in the server group, use the **max-logins** subcommand.

The following example shows the RADIUS attribute-value (AV) pairs for the maximum users and maximum logins parameters:

```
ipsec:max-users=1000
ipsec:max-logins=1
```

The **max-users** and **max-logins** commands can be enabled together or individually to control the usage of resources by any groups or individuals.

If you use a RADIUS server, such as a CiscoSecure access control server (ACS), it is recommended that you enable this session control on the RADIUS server if the functionality is provided. In this way, usage can be controlled across a number of servers by one central repository. When enabling this feature on the router itself, only connections to groups on that specific device are monitored, and load-sharing scenarios are not accurately accounted for.

Examples

The following example shows how to define group policy information for Mode Configuration push. In this example, the first group name is “cisco” and the second group name is “default.” Thus, the default policy will be enforced for all users who do not offer a group name that matches “cisco.”

```
crypto isakmp client configuration group cisco
 key cisco
 dns 10.2.2.2 10.2.2.3
 wins 10.6.6.6
 domain cisco.com
 pool fred
 acl 199
```

```
!
crypto isakmp client configuration group default
 key cisco
 dns 10.2.2.2 10.3.2.3
 pool fred
 acl 199
```

Related Commands

Command	Description
access-restrict	Ties a particular VPN group to a specific interface for access to the Cisco IOS gateway and the services it protects.
acl	Configures split tunneling.
backup-gateway	Configures a server to "push down" a list of backup gateways to the client.
browser-proxy	Applies browser-proxy parameter settings to a group.
crypto isakmp keepalive	Adds the Firewall-Are-U-There attribute to the server group if your PC is running the Black Ice or Zone Alarm personal firewalls.
dns	Specifies the primary and secondary DNS servers.
domain (isakmp-group)	Specifies the DNS domain to which a group belongs.
firewall are-u-there	Adds the Firewall-Are-U-There attribute to the server group if your PC is running the Black Ice or Zone Alarm personal firewalls.
firewall policy	Specifies the CPP firewall policy push name for the crypto ISAKMP client configuration group on a local AAA server.
group-lock	Allows you to enter your Xauth username, including the group name, when preshared key authentication is used with IKE.
include-local-lan	Configures the Include-Local-LAN attribute to allow a nonsplit-tunneling connection to access the local subnetwork at the same time as the client.
key (isakmp-group)	Specifies the IKE preshared key for Group-Policy attribute definition.
max-logins	Limits the number of simultaneous logins for users in a specific server group.
max-users	Limits the number of connections to a specific server group.
pool (isakmp-group)	Defines a local pool address.
save-password	Saves your Xauth password locally on your PC.
set aggressive-mode client-endpoint	Specifies the Tunnel-Client-Endpoint attribute within an ISAKMP peer configuration.

crypto isakmp client firewall

To define the Central Policy Push (CPP) firewall policypush on a server, use the **crypto isakmp client firewall** command in global configuration mode. To remove the CPP that was configured, use the **no** form of this command.

crypto isakmp client firewall {*policy-name*} {**required** | **optional**} {*firewall-type*}

nocrypto isakmp client firewall {*policy-name*} {**required** | **optional}** {*firewall-type*}

Syntax Description

policy-name	Uniquely identifies a policy. A policy name can be associated with an Easy VPN client group configuration on the server (local group configuration) or on the authentication, authorization, and accounting (AAA) server.
required	Policy is mandatory. If the CPP policy is defined as mandatory and is included in the Easy VPN server configuration, the tunnel setup is allowed only if the Cisco VPN Client confirms this policy. If the policy is not confirmed, the tunnel is terminated.
optional	Policy is optional. If the CPP policy is defined as optional and is included in the Easy VPN server configuration, the tunnel setup continues even if the Cisco VPN Client does not confirm the defined policy.
firewall-type	Type of firewall. See Table 24 for a list of acceptable firewall types.

Command Default

CPP is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Table 24 lists firewall types that may be used for the *firewall-type* argument.

Table 24 Acceptable Firewall Types

Firewall Type
Cisco-Integrated-firewall (central-policy-push)
Cisco-Security-Agent (check-presence)
Zonelabs-Zonealarm (both)
Zonelabs-ZonealarmPro (both)

Examples

The following example defines the CPP policy name as “hw-client-g-cpp.” The “Cisco-Security-Agent” policy type is mandatory. The CPP inbound list is “192” and the outbound list is “sample”:

```
crypto isakmp client firewall hw-client-g-cpp required Cisco-Security-Agent
 policy central-policy-push access-list in 192
 policy central-policy-push access-list out sample
 policy check-presence
```

Related Commands

Command	Description
policy	Specifies the CPP policy.

crypto isakmp default policy

To enable default policies for Internet Security Association and Key Management Protocol (ISAKMP) protection suite, use the **crypto isakmp default policy** command in global configuration mode. To disable the default IKE policies, use the **no** form of this command.

crypto isakmp default policy

no crypto isakmp default policy

Syntax Description

This command has no arguments or keywords.

Command Default

The default ISAKMP policies are enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

If you have neither manually configured ISAKMP policies with the **crypto isakmp policy** command nor issued the **no crypto isakmp default policy** command, IPsec will use the default ISAKMP policies to negotiate IKE proposals. There are eight default ISAKMP default policies supported (see Table 25). The default ISAKMP policies define the following policy set parameters:

- The priority, 65507–65514, where 65507 is the highest priority and 65514 is the lowest priority.
- The authentication method, Rivest, Shamir, and Adelman (RSA) or preshared keys (PSK).
- The encryption method, Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES).
- The hash function, Secure Hash Algorithm (SHA-1) or Message-Digest algorithm 5 (MD5).
- The Diffie-Hellman (DH) group specification DH2 or DH5.
  - DH2 specifies the 768-bit Diffie-Hellman group.
  - DH5 specifies the 1536-bit Diffie-Hellman group.

Table 25 Default ISAKMP Policies

Priority	Authentication	Encryption	Hash	Diffie-Hellman
65507	RSA	AES	SHA	DH5
65508	PSK	AES	SHA	DH5
65509	RSA	AES	MD5	DH5

Table 25 Default ISAKMP Policies (continued)

Priority	Authentication	Encryption	Hash	Diffie-Hellman
65510	PSK	AES	MD5	DH5
65511	RSA	3DES	SHA	DH2
65512	PSK	3DES	SHA	DH2
65513	RSA	3DES	MD5	DH2
65514	PSK	3DES	MD5	DH2

Examples

The following example disables the default ISAKMP policies and shows the resulting output of the **show crypto isakmp default policy** command, which is blank:

```
Router# configure terminal
Router(config)# no crypto isakmp default policy
Router(config)# exit
Router# show crypto isakmp default policy
Router#
!There is no output since the default IKE policies have been disabled.
```

The following example enables the default ISAKMP policies and displays the resulting output of the **show crypto isakmp default policy** command. The default policies are displayed because there are no user configured policies, and the default policies have not been disabled.

```
Router# configure terminal
Router(config)# crypto isakmp default policy
Router(config)# exit
Router# show crypto isakmp default policy

Default IKE policy
Default protection suite of priority 65507
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65508
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65509
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65510
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65511
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
```

```
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65512
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65513
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65514
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
```

Related Commands

Command	Description
show crypto isakmp default policy	Displays the default ISAKMP policies currently in use.

crypto isakmp enable

To globally enable Internet Key Exchange (IKE) for your peer router, use the **crypto isakmp enable** command in global configuration mode. To disable IKE for the peer, use the **no** form of this command.

crypto isakmp enable

no crypto isakmp enable

Syntax Description

This command has no arguments or keywords.

Defaults

IKE is enabled.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

IKE is enabled by default. IKE does not have to be enabled for individual interfaces, but is enabled globally for all interfaces at the router.

If you do not want IKE to be used for your IPSec implementation, you can disable IKE for all your IP Security peers. If you disable IKE for one peer, you must disable it for all IPSec peers.

If you disable IKE, you will have to make these concessions at the peers:

- You must manually specify all the IPSec security associations (SAs) in the crypto maps at the peers. (Crypto map configuration is described in the chapter "Configuring IPSec Network Security" in the *Cisco IOS Security Configuration Guide*.)
- The IPSec SAs of the peers will never time out for a given IPSec session.
- During IPSec sessions between the peers, the encryption keys will never change.
- Anti-replay services will not be available between the peers.
- Certification authority (CA) support cannot be used.

Note Effective with Cisco IOS Release 12.3(2)T, a device is prevented from responding to Internet Security Association and Key Management Protocol (ISAKMP) by default unless there is a crypto map applied to an interface or if Easy VPN is configured.

Examples

The following example disables IKE at one peer. (The same command should be issued for all remote peers.)

```
no crypto isakmp enable
```

crypto isakmp fragmentation

To enable fragmentation of large Internet Key Exchange (IKE) packets into a series of smaller IKE packets to avoid fragmentation at the User Datagram Protocol (UDP) layer, use the **crypto isakmp fragmentation** command in global configuration mode. To disable fragmentation, use the **no** form of this command.

crypto isakmp fragmentation

no crypto isakmp fragmentation

Syntax Description

This command has no arguments or keywords.

Command Default

Fragmentation is not allowed.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T7	This command was introduced.

Usage Guidelines

Do not configure IKE fragmentation on a Cisco IOS router with Cisco Easy VPN Client versions 5.01 through 5.03. Versions earlier than version 5.01 and version 5.04 or a later release should be all right.

Note The **crypto isakmp fragmentation** command is only applicable when the IOS Router is acting as an Easy VPN server and the remote peer is a Cisco IPsec VPN client.

Examples

The following example shows that fragmentation has been enabled:

```
crypto isakmp fragmentation

crypto isakmp policy 1
  encryption 3des
crypto isakmp profile ezvpn-SW
  match group frag-clients
  vrf frags
```

crypto isakmp identity

To define the ISAKMP identity used by the router when participating in the Internet Key Exchange (IKE) protocol, use the **crypto isakmp identity** command in global configuration mode. To reset the ISAKMP identity to the default value (address), use the **no** form of this command.

crypto isakmp identity {**address** | **dn** | **hostname**}

no crypto isakmp identity

Syntax Description

address	Sets the ISAKMP identity to the IP address of the interface that is used to communicate to the remote peer during IKE negotiations.
dn	Sets the ISAKMP identity to the distinguished name (DN) of the router certificate.
hostname	Sets the ISAKMP identity to the host name concatenated with the domain name (for example, myhost.example.com).

Command Default

The IP address is used for the ISAKMP identity.

Command Modes

Global configuration

Command History

Release	Modification
11.3T	This command was introduced.
12.4(4)T	Support for IPv6 was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to specify an ISAKMP identity either by IP address, DN or host name. An ISAKMP identity is set whenever you specify preshared keys or RSA signature authentication.

The **address** keyword is typically used when only one interface (and therefore only one IP address) will be used by the peer for IKE negotiations, and the IP address is known.

The **dn** keyword should be used if the DN of a router certificate is to be specified and chosen as the ISAKMP identity during IKE processing. The **dn** keyword is used only for certificate-based authentication.

The **hostname** keyword should be used if more than one interface on the peer might be used for IKE negotiations, or if the interface's IP address is unknown (such as with dynamically assigned IP addresses).

As a general rule, you should set all peers' identities in the same way, either by IP address or by host name.

Examples

The following example uses preshared keys at two peers and sets both their ISAKMP identities to the IP address.

At the local peer (at 10.0.0.1) the ISAKMP identity is set and the preshared key is specified:

```
crypto isakmp identity address
crypto isakmp key sharedkeystring address 192.168.1.33
```

At the remote peer (at 192.168.1.33) the ISAKMP identity is set and the same preshared key is specified:

```
crypto isakmp identity address
crypto isakmp key sharedkeystring address 10.0.0.1
```

Note In the preceding example if the **crypto isakmp identity** command had not been performed, the ISAKMP identities would have still been set to IP address, the default identity.

The following example uses preshared keys at two peers and sets both their ISAKMP identities to the hostname.

At the local peer the ISAKMP identity is set and the preshared key is specified:

```
crypto isakmp identity hostname
crypto isakmp key sharedkeystring hostname RemoteRouter.example.com
ip host RemoteRouter.example.com 192.168.0.1
```

At the remote peer the ISAKMP identity is set and the same preshared key is specified:

```
crypto isakmp identity hostname
crypto isakmp key sharedkeystring hostname LocalRouter.example.com
ip host LocalRouter.example.com 10.0.0.1 10.0.0.2
```

In the example, hostnames are used for the peers' identities because the local peer has two interfaces that might be used during an IKE negotiation.

In the example the IP addresses are also mapped to the hostnames; this mapping is not necessary if the routers' hostnames are already mapped in DNS.

Related Commands

Command	Description
crypto ipsec security-association lifetime	Specifies the authentication method within an IKE policy.
crypto isakmp key	Configures a preshared authentication key.

crypto isakmp invalid-spi-recovery

To initiate the Internet Key Exchange (IKE) security association (SA) to notify the receiving IP Security (IPSec) peer that there is an "Invalid SPI" error, use the **crypto isakmp invalid-spi-recovery** command in global configuration mode. To disable the notification process, use the **no** form of this command.

crypto isakmp invalid-spi-recovery

no crypto isakmp invalid-spi-recovery

Syntax Description

This command has no arguments or keywords.

Defaults

The IKE notification process is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command allows you to configure your router so that when an invalid security parameter index error (shown as "Invalid SPI") occurs, an IKE SA is initiated. The "IKE" module, which serves as a checkpoint in the IPSec session, recognizes the "Invalid SPI" situation. The IKE module then sends an "Invalid Error" message to the packet-receiving peer so that synchronization of the security association databases (SADBs) of the two peers can be attempted. As soon as the SADBs are resynchronized, packets are no longer dropped.

Note SPI recovery initiates a new IKE SA only for static peers.

Caution Using this command to initiate an IKE SA to notify an IPSec peer of an "Invalid SPI" error can result in a denial-of-service (DoS) attack.

Examples

The following example shows that the IKE module process has been initiated to notify the receiving peer that there is an "Invalid SPI" error:

```
Router (config)# crypto isakmp invalid-spi-recovery
```

crypto isakmp keepalive

To allow the gateway to send dead peer detection (DPD) keepalive messages to the peer, use the **crypto isakmp keepalive** command in global configuration mode. To disable keepalives, use the **no** form of this command.

crypto isakmp keepalive *seconds* [*retry-seconds*] [**periodic | on-demand**]

no crypto isakmp keepalive *seconds* [*retry-seconds*] [**periodic | on-demand**]

Syntax Description

seconds	When the **periodic** keyword is used, this argument is the number of seconds between DPD messages; the range is from 10 to 3600 seconds. When the **on-demand** keyword is used, this argument is the number of seconds during which traffic is not received from the peer before DPD retry messages are sent if there is data (IPSec) traffic to send; the range is from 10 to 3600 seconds. **Note** If you do not specify a time interval, an error message appears.
retry-seconds	(Optional) Number of seconds between DPD retry messages if the DPD retry message is missed by the peer; the range is from 2 to 60 seconds. Once 1 DPD message is missed by the peer, the router moves to a more aggressive state and sends the DPD retry message at the faster retry interval, which is the number of seconds between DPD retries if the DPD message is missed by the peer. The default DPD retry message is sent every 2 seconds. Five aggressive DPD retry messages can be missed before the tunnel is marked as down. **Note** To configure DPD with IPsec High Availability (HA), the recommendation is to use a value other than the default (which is 2 seconds). A keepalive timer of 10 seconds with 5 retries seems to work well with HA because of the time that it takes for the router to get into active mode.
periodic	(Optional) DPD messages are sent at regular intervals.
on-demand	(Optional) The default behavior. DPD retries are sent on demand. **Note** Because this option is the default, the **on-demand** keyword does not appear in configuration output.

Command Default

No DPD messages are sent.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.3(7)T	The **periodic** and **on-demand** keywords were added.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use the **crypto isakmp keepalive** command to enable the gateway to send DPD messages to the peer. DPD is a keepalives scheme that allows the router to query the liveliness of its Internet Key Exchange (IKE) peer.

Use the **periodic** keyword to configure your router so that DPD messages are "forced" at regular intervals. This forced approach results in earlier detection of dead peers than with the on-demand approach. If you do not configure the periodic option, the router defaults to the on-demand approach.

Note When the **crypto isakmp keepalive** command is configured, the Cisco IOS software negotiates the use of Cisco IOS keepalives or DPD, depending on which protocol the peer supports.

Note Cisco IOS VPN Client connections are not supported if you configure the **crypto isakmp keepalive** command with the **periodic** keyword on a Cisco IOS device.

Examples

The following example shows how to configure DPD messages to be sent every 60 seconds and a DPD retry message every 3 seconds between retries if the peer does not respond one time:

```
crypto isakmp keepalive 60 3
```

The 60 indicates that a keepalive or DPD message is sent every 60 seconds. Once a DPD message is missed by the peer, the router moves to a more aggressive state, sending DPD retry messages every 3 seconds. After 5 aggressive DPD retries, the tunnel is marked as down.

In this example, if the router has sent a DPD message at time *x* and has not received a response within *x* + 60, then the DPD retry is sent again at *x* + 60 and then aggressively at time intervals of *x* + 63, *x* + 66, *x* + 69, and *x* + 72. At *x* + 75, a decision is made by the router to bring down the tunnel and DELETE payload is sent to the peer. The DPD retry message is not sent at *x* + 75 and only DELETE payload is sent. Therefore, the number of aggressive DPD retry messages that can be missed before marking the tunnel as down is 5 (sent at intervals *x* + 60, *x* + 63, *x*+66, *x* + 69, and *x* + 72).

The following example shows that periodic DPD messages are to be sent at intervals of 10 seconds:

```
crypto isakmp keepalive 10 periodic
```

The following example shows that the above periodic behavior is being disabled:

```
crypto isakmp keepalive 10 on-demand
```

The following example shows that DPD has been configured with IPsec HA. The number of seconds between DPD messages is 10, and the number of seconds between DPD retries is 5. DPD messages are to be sent at regular intervals.

```
crypto isakmp keepalive 10 5 periodic
```

Related Commands

Command	Description
acl	Configures split tunneling.

crypto isakmp key

To configure a preshared authentication key, use the **crypto isakmp key** command in global configuration mode. To delete a preshared authentication key, use the **no** form of this command.

crypto isakmp key *enc-type-digit keystring* {**address** *peer-address* [*mask*] | **ipv6** *ipv6-address/ipv6-prefix* | **hostname** *hostname*} [**no-xauth**]

no crypto isakmp key *enc-type-digit keystring* {**address** *peer-address* [*mask*] | **ipv6** *ipv6-address/ipv6-prefix* | **hostname** *hostname*} [**no-xauth**]

Syntax Description

enc-type-digit	Specifies whether the password to be used is encrypted or unencrypted. • 0—Specifies that an unencrypted password follows. • 6—Specifies that an encrypted password follows.
keystring	Specifies the preshared key. Use any combination of alphanumeric or special characters up to 128 bytes. Special characters include the following: !?"#$%&'()*+,-./:;<=>@[\]^_`~. (Type "CTRL-V" before the "?" symbol to avoid invoking help.) This preshared key must be identical at both peers.
address	Use this keyword if the remote peer Internet Security Association Key Management Protocol (ISAKMP) identity was set with its IP or IPv6 address. The *peer-address* argument specifies the IP or IPv6 address of the remote peer.
peer-address	Specifies the IP address of the remote peer.
mask	(Optional) Specifies the subnet address of the remote peer. (The argument can be used only if the remote peer ISAKMP identity was set with its IP address.)
ipv6	Specifies that an IPv6 address of a remote peer will be used.
ipv6-address	IPv6 address of the remote peer. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
ipv6-prefix	IPv6 prefix of the remote peer.
hostname *hostname*	Fully qualified domain name (FQDN) of the peer. The **hostname** keyword and *hostname* argument are not supported by IPv6.
no-xauth	(Optional) Use this keyword if router-to-router IP Security (IPSec) is on the same crypto map as a Virtual Private Network (VPN)-client-to-Cisco-IOS IPSec. This keyword prevents the router from prompting the peer for extended authentication (Xauth) information (username and password).

Command Default

There is no default preshared authentication key.

Command Modes

Global configuration

Command History

Release	Modification
11.3T	This command was introduced.
12.1(1)T	The *mask* argument was added.
12.2(4)T	The **no-xauth** keyword was added.
12.3(2)T	This command was modified so that output shows that the preshared key is either encrypted or unencrypted.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(4)T	The **ipv6** keyword and the *ipv6-address* and *ipv6-prefix* arguments were added.

Usage Guidelines

You must use this command to configure a key whenever you specify preshared keys in an Internet Key Exchange (IKE) policy; you must enable this command at both peers.

If an IKE policy includes preshared keys as the authentication method, these preshared keys must be configured at both peers—otherwise the policy cannot be used (the policy will not be submitted for matching by the IKE process). The **crypto isakmp key** command is the second task required to configure the preshared keys at the peers. (The first task is accomplished using the **crypto isakmp identity** command.)

Use the **address** keyword if the remote peer ISAKMP identity was set with its IP address.

With the **address** keyword, you can also use the *mask* argument to indicate the remote peer ISAKMP identity will be established using the preshared key only. If the *mask* argument is used, preshared keys are no longer restricted between two users.

Note If you specify *mask*, you must use a subnet address. (The subnet address 0.0.0.0 is not recommended because it encourages group preshared keys, which allow all peers to have the same group key, thereby reducing the security of your user authentication.)

When using IKE main mode, preshared keys are indexed by IP address only because the identity payload has not yet been received. This means that the hostname keyword in the identity statement is not used to look up a preshared key and will be used only when sending and processing the identity payloads later in the main mode exchange. The identity keyword can be used when preshared keys are used with IKE aggressive mode, and keys may be indexed by identity types other than IP address as the identity payload is received in the first IKE aggressive mode packet.

If **crypto isakmp identity hostname** is configured as identity, the preshared key *must* be configured with the peer's IP address for the process to work when using IKE in main mode.

Use the **no-xauth** keyword to prevent the router from prompting the peer for Xauth information (username and password). This keyword disables Xauth for static IPSec peers. The **no-xauth** keyword should be enabled when configuring the preshared key for router-to-router IPSec—not VPN-client-to-Cisco-IOS IPSec.

Output for the **crypto isakmp key** command will show that the preshared key is either encrypted or unencrypted. An output example for an unencrypted preshared key would be as follows:

```
crypto isakmp key test123 address 10.1.0.1
```

An output example for a type 6 encrypted preshared key would be as follows:

```
crypto isakmp key 6 RHZE[JACMUI\bcbTdELISAAB address 10.1.0.1
```

Examples

In the following example, the remote peer "RemoteRouter" specifies an ISAKMP identity by address:

```
crypto isakmp identity address
```

Now, the preshared key must be specified at each peer.

In the following example, the local peer specifies the preshared key and designates the remote peer by its IP address and a mask:

```
crypto isakmp key 0 sharedkeystring address 172.21.230.33  255.255.255.255
```

In the following example for IPv6, the peer specifies the preshared key and designates the remote peer with an IPv6 address:

```
crypto isakmp key 0 my-preshare-key-0 address ipv6 3ffe:1001::2/128
```

Related Commandsl

Command	Description
crypto ipsec security-association lifetime	Specifies the authentication method within an IKE policy.
crypto isakmp identity	Defines the identity the router uses when participating in the IKE protocol.
ip host	Defines a static host name-to-address mapping in the host cache.

crypto isakmp nat keepalive

To allow an IP Security (IPSec) node to send Network Address Translation (NAT) keepalive packets, use the **crypto isakmp nat keepalive** command in global configuration mode. To disable NAT keepalive packets, use the **no** form of this command.

crypto isakmp nat keepalive *seconds*

no crypto isakmp nat keepalive

Syntax Description

seconds	Number of seconds between keepalive packets; the range is between 5 and 3600 seconds.

Defaults

NAT keepalive packets are not sent.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

The **crypto isakmp nat keepalive** command allows users to keep the dynamic NAT mapping alive during a connection between two peers. A NAT keepalive beat is sent if IPSec does not send or receive a packet within a specified time period.

If this command is enabled, users should ensure that the idle value is shorter than than the NAT mapping expiration time.

Note When the timer is modified, it is modified for every Internet Security Association Key Management Protocol (ISAKMP) security association (SA) when the keepalive for that SA is sent based on the existing timer.

Note A five-percent jitter mechanism value is applied to the timer to avoid security association rekey collisions. If there are many peer routers, and the timer is configured too low, then the router can experience high CPU usage.

Examples

The following example shows how to enable NAT keepalives to be sent every 20 seconds:

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key 1234 address 209.165.202.130
crypto isakmp nat keepalive 20
!
```

```
crypto ipsec transform-set t2 esp-des esp-sha-hmac
no crypto engine accelerator
!
crypto map test2 10 ipsec-isakmp
 set peer 209.165.202.130
 set transform-set t2
 match address 101
```

crypto isakmp peer

To enable an IP Security (IPSec) peer for Internet Key Exchange (IKE) querying of authentication, authorization, and accounting (AAA) for tunnel attributes in aggressive mode, use the **crypto isakmp peer** command in global configuration mode. To disable this functionality, use the **no** form of this command.

crypto isakmp peer {**address** {*ipv4-address* | **ipv6** *ipv6-address*} | **hostname** *fqdn-hostname*}

no crypto isakmp peer {**address** {*ipv4-address* | **ipv6** *ipv6-address*} | **hostname** *fqdn-hostname*}

Syntax Description

address *ip-address*	Address of the peer router.
ipv4-address	IPv4 address of the peer router.
ipv6 *ipv6-address*	IPv6 address of the peer router.
hostname	Hostname of the peer router.
fqdn-hostname	Fully qualified domain name (FQDN) of the peer router.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(15)T	The **vrf** keyword and *fvrf-name* argument were added.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(4)T	The **ipv6** keyword and *ipv6-address* argument were added.

Usage Guidelines

After enabling this command, you can use the **set aggressive-mode client-endpoint** and **set aggressive-mode password** commands to specify RADIUS tunnel attributes in the Internet Security Association and Key Management Protocol (ISAKMP) peer policy for IPSec peers.

Instead of keeping your preshared keys on the hub router, you can scale your preshared keys by storing and retrieving them from an AAA server. The preshared keys are stored in the AAA server as Internet Engineering Task Force (IETF) RADIUS tunnel attributes and are retrieved when a user tries to "speak" to the hub router. The hub router retrieves the preshared key from the AAA server and the spokes (the users) initiate aggressive mode to the hub by using the preshared key that is specified in the ISAKMP peer policy as a RADIUS tunnel attribute.

Examples

The following example shows how to initiate aggressive mode using RADIUS tunnel attributes:

```
crypto isakmp peer ip-address 209.165.200.230 vrf vpn1
 set aggressive-mode client-endpoint user-fqdn user@cisco.com
 set aggressive-mode password cisco123
```

Related Commands

Command	Description
crypto map isakmp authorization list	Enables IKE querying of AAA for tunnel attributes in aggressive mode.
set aggressive-mode client-endpoint	Specifies the Tunnel-Client-Endpoint attribute within an ISAKMP peer configuration.
set aggressive-mode password	Specifies the Tunnel-Password attribute within an ISAKMP peer configuration.

crypto isakmp policy

To define an Internet Key Exchange (IKE) policy, use the **crypto isakmp policy** command in global configuration mode. To delete an IKE policy, use the **no** form of this command.

crypto isakmp policy *priority*

no crypto isakmp policy *priority*

Syntax Description

priority	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 10,000, with 1 being the highest priority and 10,000 the lowest.

Command Default

Default IKE policies are in use.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3T	This command was introduced.
12.4(4)T	Support for IPv6 was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	The command default was modified. Support for eight default IKE (ISAKMP) policies was added.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

IKE policies define a set of parameters to be used during the IKE negotiation. Use this command to specify the parameters to be used during an IKE negotiation. (These parameters are used to create the IKE security association [SA].)

This command invokes the Internet Security Association Key Management Protocol (ISAKMP) policy configuration (config-isakmp) command mode. While in the ISAKMP policy configuration command mode, some of the commands for which you can specify parameters are as follows:

- **authentication**; default = RSA signatures
- **encryption (IKE policy)**; default = 56-bit DES-CBC
- **group (IKE policy)**; default = 768-bit Diffie-Hellman
- **hash (IKE policy)**; default = SHA-1
- **lifetime (IKE policy)**; default = 86,400 seconds (one day)

If you do not specify any given parameter, the default value will be used for that parameter.

To exit the config-isakmp command mode, type **exit**.

You can configure multiple IKE policies on each peer participating in IPsec. When the IKE negotiation begins, it tries to find a common policy configured on both peers, starting with the highest priority policies as specified on the remote peer.

Examples

The following example shows how to manually configure two policies for the peer:

```
crypto isakmp policy 15
 hash md5
 authentication rsa-sig
 group 2
 lifetime 5000
crypto isakmp policy 20
 authentication pre-share
 lifetime 10000
```

The above configuration results in the following policies:

```
Router# show crypto isakmp policy

Protection suite priority 15
    encryption algorithm:DES - Data Encryption Standard (56 bit keys)
    hash algorithm:Message Digest 5
    authentication method:Rivest-Shamir-Adleman Signature
    Diffie-Hellman Group:#2 (1024 bit)
    lifetime:5000 seconds, no volume limit
Protection suite priority 20
    encryption algorithm:DES - Data Encryption Standard (56 bit keys)
    hash algorithm:Secure Hash Standard
    authentication method:preshared Key
    Diffie-Hellman Group:#1 (768 bit)
    lifetime:10000 seconds, no volume limit
Default protection suite
    encryption algorithm:DES - Data Encryption Standard (56 bit keys)
    hash algorithm:Secure Hash Standard
    authentication method:Rivest-Shamir-Adleman Signature
    Diffie-Hellman Group:#1 (768 bit)
    lifetime:86400 seconds, no volume limit
```

The following sample output from the **show crypto isakmp policy** command displays the default IKE policies when the manually configured IKE policies with priorities 15 and 20 have been removed.

```
Router(config)# no crypto isakmp policy 15
Router(config)# no crypto isakmp policy 20
Router(config)# exit
R1# show crypto isakmp policy

Default IKE policy
Protection suite of priority 65507
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65508
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65509
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Message Digest 5
```

```
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65510
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65511
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65512
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65513
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65514
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
```

Related Commands

Command	Description
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
group (IKE policy)	Specifies the Diffie-Hellman group identifier within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
show crypto isakmp default policy	Displays the default IKE (ISAKMP) policies currently in use.
show crypto isakmp policy	Displays the parameters for each IKE policy.

crypto isakmp profile

To define an Internet Security Association and Key Management Protocol (ISAKMP) profile and to audit IP security (IPsec) user sessions, use the **crypto isakmp profile** command in global configuration mode. To delete a crypto ISAKMP profile, use the **no** form of this command.

crypto isakmp profile *profile-name* [**accounting** *aaa-list*]

no crypto isakmp profile *profile-name* [**accounting** *aaa-list*]

Syntax Description

profile-name	Name of the user profile. To associate a user profile with the RADIUS server, the user profile name must be identified.
accounting *aaa-list*	(Optional) Name of a client accounting list.

Command Defaults

No profile exists if the command is not used.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(2)T	Support for dynamic virtual tunnel interfaces was added.
12.4(4)T	Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Defining an ISAKMP Profile

An ISAKMP profile can be viewed as a repository of Phase 1 and Phase 1.5 commands for a set of peers. The Phase 1 configuration includes commands to configure such things as keepalive, identity matching, and the authorization list. The Phase 1.5 configuration includes commands to configure such things as extended authentication (Xauth) and mode configuration.

The peers are mapped to an ISAKMP profile when their identities are matched (as given in the identification [ID] payload of the Internet Key Exchange [IKE]) against the identities defined in the ISAKMP profile. To uniquely map to an ISAKMP profile, no two ISAKMP profiles should match the same identity. If the peer identity is matched in two ISAKMP profiles, the configuration is invalid. Also, there must be at least one **match identity** command defined in the ISAKMP profile for it to be complete.

After enabling this command and entering ISAKMP profile configuration mode, you can configure the following commands:

- **accounting**—Enables authentication, authorization, and accounting (AAA) accounting.
- **ca trust-point**—Specifies certificate authorities.
- **client**—Specifies client configuration settings.

- **default**—Lists subcommands for the **crypto isakmp profile** command.
- **description**—Specifies a description of this profile.
- **initiate mode**—Initiates a mode.
- **isakmp authorization**—ISAKMP authorization parameters.
- **keepalive**—Sets a keepalive interval.
- **keyring**—Specifies a keyring.
- **local-address**—Specifies the interface to use as the local address of this ISAKMP profile.
- **match**—Matches the values of the peer.
- **qos-group**—Applies a quality of service (QoS) policy class map for this profile.
- **self-identity**—Specifies the identity.
- **virtual-template**—Specifies the virtual template for the dynamic interface.
- **vrf**—Specifies the Virtual Private Network routing and forwarding (VRF) instance to which the profile is related.

Auditing IPSec User Sessions

Use this command to audit multiple user sessions that are terminating on the IPSec gateway.

Note The **crypto isakmp profile** command and the **crypto map (global IPSec)** command are mutually exclusive. If a profile is present (the **crypto isakmp profile** command has been used), with no accounting configured but with the global command present (the **crypto isakmp profile** command without the **accounting** keyword), accounting will occur using the attributes in the global command.

Dynamic Virtual Tunnel Interfaces

Support for dynamic virtual tunnel interfaces allows for the virtual profile to be mapped into a specified virtual template.

Examples

ISAKAMP Profile Matching Peer Identities Example

The following example shows how to define an ISAKMP profile and match the peer identities:

```
crypto isakmp profile vpnprofile
 match identity address 10.76.11.53
```

ISAKAMP Profile with Accounting Example

The following accounting example shows that an ISAKMP profile is configured:

```
aaa new-model
!
!
aaa authentication login cisco-client group radius
aaa authorization network cisco-client group radius
aaa accounting network acc start-stop broadcast group radius
aaa session-id common
!
crypto isakmp profile cisco
vrf cisco
match identity group cclient
 client authentication list cisco-client
```

```
 isakmp authorization list cisco-client
 client configuration address respond
 accounting acc
!
crypto dynamic-map dynamic 1
 set transform-set aswan
 set isakmp-profile cisco
 reverse-route
!
!
radius-server host 172.16.1.4 auth-port 1645 acct-port 1646
radius-server key nsite
```

Related Commands

Command	Description
crypto map (global IPsec)	Enters crypto map configuration mode and creates or modifies a crypto map entry, creates a crypto profile that provides a template for configuration of dynamically created crypto maps, or configures a client accounting list.
debug crypto isakmp	Displays messages about IKE events.
match identity	Matches an identity from a peer in an ISAKMP profile.
tunnel protection	Associates a tunnel interface with an IP Security (IPsec) profile.
virtual template	Specifies which virtual template to be used to clone virtual access interfaces.

crypto key decrypt rsa

To delete the encrypted RSA key and leave only the unencrypted key on the running router, use the **crypto key decrypt rsa** command in global configuration mode.

crypto key decrypt [**write**] **rsa** [**name** *key-name*] **passphrase** *passphrase*

Syntax Description

write	(Optional) Clear text (unencrypted) key is immediately written to NvRAM. If the **write** keyword is not issued, the configuration must be manually written to NvRAM; otherwise, the key will remain encrypted the next time the router is reloaded.
name *key-name*	(Optional) Name of the RSA key pair that is to be decrypted.
passphrase *passphrase*	Passphrase that is used to decrypt the RSA key. The passphrase must match the passphrase that was specified via the **crypto key encrypt rsa** command.

Defaults

The private key running on the router is encrypted.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.

Usage Guidelines

Use the **crypto key decrypt rsa** command to store the decrypted private key in NvRAM the next time NvRAM is written (which is immediately if the **write** keyword is issed).

Examples

The following example shows how to decrypt the RSA key “pki1-72a.cisco.com”:

```
Router(config)# crypto key decrypt write rsa name pki1-72a.cisco.com passphrase cisco1234
```

Related Commands

Command	Description
crypto key encrypt rsa	Encrypts the RSA private key.
show crypto key mypubkey rsa	Displays the RSA public keys of your router.

crypto key encrypt rsa

To encrypt the RSA private key, use the **crypto key encrypt rsa** command in global configuration mode.

crypto key encrypt [**write**] **rsa** [**name** *key-name*] **passphrase** *passphrase*

Syntax Description

write	(Optional) Router configuration is immediately written to NVRAM. If the **write** keyword is not issued, the configuration must be manually written to NvRAM; otherwise, the encrypted key will be lost next time the router is reloaded.
name *key-name*	(Optional) Name of the RSA key pair that is to be encrypted. If a key name is not specified, the default key name, *routername.domainname*, is used.
passphrase *passphrase*	Passphrase that is used to encrypt the RSA key. To access the RSA key pair, the passphrase must be specified.

Defaults

RSA keys are not encrypted.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.

Usage Guidelines

The private key is encrypted (protected) via the specified passphrase. After the key is protected, it may continue to be used by the router; that is Internet Key Exchange (IKE) tunnels and encrypted key export attempts should continue to work because the key remains "unlocked."

To lock the key, which can be used to disable the router, issue the **crypto key lock rsa** privileged EXEC command. (When you lock the encrypted key, all functions which use the locked key are disabled.)

Examples

The following example shows how to encrypt the RSA key "pki1-72a.cisco.com." Thereafter, the **show crypto key mypubkey rsa** command is issued to verify that the RSA key is encrypted and unlocked.

```
Router(config)# crypto key encrypt rsa name pki1-72a.cisco.com passphrase cisco1234
Router(config)# exit
Router# show crypto key mypubkey rsa
```

```
% Key pair was generated at:00:15:32 GMT Jun 25 2003
Key name:pki1-72a.cisco.com
Usage:General Purpose Key
*** The key is protected and UNLOCKED. ***
Key is not exportable.
Key Data:
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E0CC9A 1D23B52C
CD00910C ABD392AE BA6D0E3F FC47A0EF 8AFEE340 0EC1E62B D40E7DCC
23C4D09E
03018B98 E0C07B42 3CFD1A32 2A3A13C0 1FF919C5 8DE9565F 1F020301 0001
% Key pair was generated at:00:15:33 GMT Jun 25 2003
Key name:pki1-72a.cisco.com.server
Usage:Encryption Key
Key is exportable.
Key Data:
307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00D3491E 2A21D383
854D7DA8 58AFBDAC 4E11A7DD E6C40AC6 66473A9F 0C845120 7C0C6EC8 1FFF5757
3A41CE04 FDCB40A4 B9C68B4F BC7D624B 470339A3 DE739D3E F7DDB549 91CD4DA4
DF190D26 7033958C 8A61787B D40D28B8 29BCD0ED 4E6275C0 6D020301 0001
Router#
```

Related Commands

Command	Description
crypto key decrypt rsa	Deletes the encrypted RSA key and leaves only the unencrypted key on the running router.
crypto key lock rsa	Locks the RSA private key in a router.
show crypto key mypubkey rsa	Displays the RSA public keys of your router.

crypto key export rsa pem

To export Rivest, Shamir, and Adelman (RSA) keys in privacy-enhanced mail (PEM)-formatted files, use the **crypto key export rsa pem** command in global configuration mode.

crypto key export rsa *key-label* **pem** {**terminal** | **url** *url*} {**3des** | **des**} *passphrase*

Syntax Description

rsa *key-label*	Name of the RSA key pair that will be exported. The *key-label* argument must match the key pair name that was specified via the **crypto key generate rsa** command.
terminal	RSA key pair will be displayed in PEM format on the console terminal.
url *url*	URL of the file system where your router should export the RSA key pair.
3des	Export the RSA key pair using the Triple Data Encryption Standard (3DES) encryption algorithm.
des	Export the RSA key pair using the DES encryption algorithm.
passphrase	Passphrase that is used to encrypt the PEM file for import. **Note** The passphrase can be any phrase that is at least eight characters in length; it can include spaces and punctuation, excluding the question mark (?), which has special meaning to the Cisco IOS parser.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The **crypto key export rsa pem** command allows you to export RSA key pairs in PEM-formatted files. The PEM files can then be imported back into a Cisco IOS router or other public key infrastructure (PKI) applications.

Note Before you can export a RSA key pair in a PEM file, ensure that the RSA key pair is exportable. To generate an exportable RSA key pair, issue the **crypto key generate rsa** command and specify the **exportable** keyword.

Examples

The following example shows how to generate, export, bring the key back (import), and verify the status of the RSA key pair “mycs”:

```
! Generate the key pair
!
Router(config)# crypto key generate rsa general-purpose label mycs exportable
```

```
The name for the keys will be: mycs
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys ...[OK]
!
! Archive the key pair to a remote location, and use a good password.
!
Router(config)# crypto key export rsa mycs pem url nvram: 3des PASSWORD
% Key name: mycs
Usage: General Purpose Key
Exporting public key...
Destination filename [mycs.pub]?
Writing file to nvram:mycs.pub
Exporting private key...
Destination filename [mycs.prv]?
Writing file to nvram:mycs.prv
!
! Import the key as a different name.
!
Router(config)# crypto key import rsa mycs2 pem url nvram:mycs PASSWORD
% Importing public key or certificate PEM file...
Source filename [mycs.pub]?
Reading file from nvram:mycs.pub
% Importing private key PEM file...
Source filename [mycs.prv]?
Reading file from nvram:mycs.prv% Key pair import succeeded.
!
! After the key has been imported, it is no longer exportable.
!
! Verify the status of the key.
!
Router# show crypto key mypubkey rsa

% Key pair was generated at: 18:04:56 GMT Jun 6 2003
Key name: mycs
Usage: General Purpose Key
Key is exportable.
Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00E65253
  9C30C12E 295AB73F B1DF9FAD 86F88192 7D4FA4D2 8BA7FB49 9045BAB9 373A31CB
  A6B1B8F4 329F2E7E 8A50997E AADBCFAA 23C29E19 C45F4F05 DBB2FA51 4B7E9F79
  A1095115 759D6BC3 5DFB5D7F BCF655BF 6317DB12 A8287795 7D8DC6A3 D31B2486
  C9C96D2C 2F70B50D 3B4CDDAE F661041A 445AE11D 002EEF08 F2A627A0 5B020301 0001
% Key pair was generated at: 18:17:25 GMT Jun 6 2003
Key name: mycs2
Usage: General Purpose Key
Key is not exportable.
Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00E65253
  9C30C12E 295AB73F B1DF9FAD 86F88192 7D4FA4D2 8BA7FB49 9045BAB9 373A31CB
  A6B1B8F4 329F2E7E 8A50997E AADBCFAA 23C29E19 C45F4F05 DBB2FA51 4B7E9F79
  A1095115 759D6BC3 5DFB5D7F BCF655BF 6317DB12 A8287795 7D8DC6A3 D31B2486
  C9C96D2C 2F70B50D 3B4CDDAE F661041A 445AE11D 002EEF08 F2A627A0 5B020301 0001
```

Related Commands

Command	Description
crypto key generate rsa	Generates RSA key pairs.
crypto key import rsa pem	Imports RSA keys in PEM-formatted files.

crypto key generate ec keysize

To generate Elliptic Curve (EC) key pairs, use the **crypto key generate ec keysize** command in global configuration mode.

crypto key generate ec keysize [**256** | **384**] [**label** *key-label*]

no crypto key generate ec keysize

Syntax Description

256	Specifies a 256-bit keysize.
384	Specifies a 384-bit keysize.
label *key-label*	(Optional) Specifies the name that is used for the EC key pair when they are being exported. If a key label is not specified, the fully qualified domain name (FQDN) of the router is used.

Command Default

The EC key pairs do not exist.

Command Modes

Global configuration

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

Use this command to generate EC key pairs for your Cisco device (such as a router).

Examples

The following example generates a 256-bit EC key pair with the label “Router_1_Key”.

```
Router(config)# crypto key generate ec keysize 256 label Router_1_Key
```

Related Commands

Command	Description
copy	Copies any file from a source to a destination, use the copy command in privileged EXEC mode.
crypto key generate rsa	Generates RSA keys.
crypto key storage	Sets the default storage location for RSA key pairs.
debug crypto engine	Displays debug messages about crypto engines.
hostname	Specifies or modifies the hostname for the network server.

Command	Description
ip domain-name	Defines a default domain name to complete unqualified hostnames (names without a dotted-decimal domain name).
show crypto key mypubkey rsa	Displays the RSA public keys of your router.
show crypto pki certificates	Displays information about your PKI certificate, certification authority, and any registration authority certificates.

crypto key generate rsa

To generate Rivest, Shamir, and Adelman (RSA) key pairs, use the **crypto key generate rsa** command in global configuration mode.

crypto key generate rsa [**general-keys | usage-keys | signature | encryption**] [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*] [**storage** *devicename***:**][**redundancy**][**on** *devicename***:**]

Syntax Description

general-keys	(Optional) Specifies that a general-purpose key pair will be generated, which is the default.
usage-keys	(Optional) Specifies that two RSA special-usage key pairs, one encryption pair and one signature pair, will be generated.
signature	(Optional) Specifies that the RSA public key generated will be a signature special usage key.
encryption	(Optional) Specifies that the RSA public key generated will be an encryption special usage key.
label *key-label*	(Optional) Specifies the name that is used for an RSA key pair when they are being exported. If a key label is not specified, the fully qualified domain name (FQDN) of the router is used.
exportable	(Optional) Specifies that the RSA key pair can be exported to another Cisco device, such as a router.
modulus *modulus-size*	(Optional) Specifies the IP size of the key modulus. By default, the modulus of a certification authority (CA) key is 1024 bits. The recommended modulus for a CA key is 2048 bits. The range of a CA key modulus is from 350 to 4096 bits. **Note** Effective with Cisco IOS XE Release 2.4 and Cisco IOS Release 15.1(1)T, the maximum key size was expanded to 4096 bits for private key operations. The maximum for private key operations prior to these releases was 2048 bits.
storage *devicename***:**	(Optional) Specifies the key storage location. The name of the storage device is followed by a colon (:).
redundancy	(Optional) Specifies that the key should be synchronized to the standby CA.
on *devicename***:**	(Optional) Specifies that the RSA key pair will be created on the specified device, including a Universal Serial Bus (USB) token, local disk, or NVRAM. The name of the device is followed by a colon (:). Keys created on a USB token must be 2048 bits or less.

Command Default

RSA key pairs do not exist.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(8)T	The *key-label* argument was added.
12.2(15)T	The **exportable** keyword was added.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(4)T	The **storage** keyword and *devicename***:** argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The **storage** keyword and *devicename***:** argument were implemented on the Cisco 7200VXR NPE-G2 platform. The **signature**, **encryption** and **on** keywords and *devicename***:** argument were added.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.
XE 2.4	The maximum RSA key size was expanded from 2048 to 4096 bits for private key operations.
15.0(1)M	This command was modified. The **redundancy** keyword was introduced.
15.1(1)T	This command was modified. The range value for the **modulus** keyword value is extended from 360 to 2048 bits to 360 to 4096 bits.

Usage Guidelines

Use this command to generate RSA key pairs for your Cisco device (such as a router).

RSA keys are generated in pairs—one public RSA key and one private RSA key.

If your router already has RSA keys when you issue this command, you will be warned and prompted to replace the existing keys with new keys.

Note Before issuing this command, ensure that your router has a hostname and IP domain name configured (with the **hostname** and **ip domain-name** commands). You will be unable to complete the **crypto key generate rsa** command without a hostname and IP domain name. (This situation is not true when you generate only a named key pair.)

Note Secure Shell (SSH) may generate an additional RSA key pair if you generate a key pair on a router having no RSA keys. The additional key pair is used only by SSH and will have a name such as {*router_FQDN*}.server. For example, if a router name is "router1.cisco.com," the key name is "router1.cisco.com.server."

This command is not saved in the router configuration; however, the RSA keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device) the next time the configuration is written to NVRAM.

Note If the configuration is not saved to NVRAM, the generated keys are lost on the next reload of the router.

There are two mutually exclusive types of RSA key pairs: special-usage keys and general-purpose keys. When you generate RSA key pairs, you will be prompted to select either special-usage keys or general-purpose keys.

Special-Usage Keys

If you generate special-usage keys, two pairs of RSA keys will be generated. One pair will be used with any Internet Key Exchange (IKE) policy that specifies RSA signatures as the authentication method, and the other pair will be used with any IKE policy that specifies RSA encrypted keys as the authentication method.

A CA is used only with IKE policies specifying RSA signatures, not with IKE policies specifying RSA-encrypted nonces. (However, you could specify more than one IKE policy and have RSA signatures specified in one policy and RSA-encrypted nonces in another policy.)

If you plan to have both types of RSA authentication methods in your IKE policies, you may prefer to generate special-usage keys. With special-usage keys, each key is not unnecessarily exposed. (Without special-usage keys, one key is used for both authentication methods, increasing the exposure of that key.)

General-Purpose Keys

If you generate general-purpose keys, only one pair of RSA keys will be generated. This pair will be used with IKE policies specifying either RSA signatures or RSA encrypted keys. Therefore, a general-purpose key pair might get used more frequently than a special-usage key pair.

Named Key Pairs

If you generate a named key pair using the *key-label* argument, you must also specify the **usage-keys** keyword or the **general-keys** keyword. Named key pairs allow you to have multiple RSA key pairs, enabling the Cisco IOS software to maintain a different key pair for each identity certificate.

Modulus Length

When you generate RSA keys, you will be prompted to enter a modulus length. The longer the modulus, the stronger the security. However a longer modules takes longer to generate (see Table 26 for sample times) and takes longer to use.

Table 26 Sample Times by Modulus Length to Generate RSA Keys

Router	360 bits	512 bits	1024 bits	2048 bits (maximum)
Cisco 2500	11 seconds	20 seconds	4 minutes, 38 seconds	More than 1 hour
Cisco 4700	Less than 1 second	1 second	4 seconds	50 seconds

Cisco IOS software does not support a modulus greater than 4096 bits. A length of less than 512 bits is normally not recommended. In certain situations, the shorter modulus may not function properly with IKE, so we recommend using a minimum modulus of 2048 bits.

Note As of Cisco IOS Release 12.4(11)T, peer *public* RSA key modulus values up to 4096 bits are automatically supported.

The largest private RSA key modulus is 4096 bits. Therefore, the largest RSA private key a router may generate or import is 4096 bits. However, RFC 2409 restricts the private key size to 2048 bits or less for RSA encryption.

The recommended modulus for a CA is 2048 bits; the recommended modulus for a client is 2048 bits.

Additional limitations may apply when RSA keys are generated by cryptographic hardware. For example, when RSA keys are generated by the Cisco VPN Services Port Adapter (VSPA), the RSA key modulus must be a minimum of 384 bits and must be a multiple of 64.

Specifying a Storage Location for RSA Keys

When you issue the **crypto key generate rsa** command with the **storage** *devicename***:** keyword and argument, the RSA keys will be stored on the specified device. This location will supersede any **crypto key storage** command settings.

Specifying a Device for RSA Key Generation

As of Cisco IOS Release 12.4(11)T and later releases, you may specify the device where RSA keys are generated. Devices supported include NVRAM, local disks, and USB tokens. If your router has a USB token configured and available, the USB token can be used as cryptographic device in addition to a storage device. Using a USB token as a cryptographic device allows RSA operations such as key generation, signing, and authentication of credentials to be performed on the token. The private key never leaves the USB token and is not exportable. The public key is exportable.

RSA keys may be generated on a configured and available USB token, by the use of the **on** *devicename***:** keyword and argument. Keys that reside on a USB token are saved to persistent token storage when they are generated. The number of keys that can be generated on a USB token is limited by the space available. If you attempt to generate keys on a USB token and it is full you will receive the following message:

```
% Error in generating keys:no available resources
```

Key deletion will remove the keys stored on the token from persistent storage immediately. (Keys that do not reside on a token are saved to or deleted from nontoken storage locations when the **copy** or similar command is issued.)

For information on configuring a USB token, see "Storing PKI Credentials" chapter in the *Cisco IOS Security Configuration Guide*, Release 12.4T. For information on using on-token RSA credentials, see the "Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment" chapter in the *Cisco IOS Security Configuration Guide*, Release 12.4T.

Specifying RSA Key Redundancy Generation on a Device

You can specify redundancy for existing keys only if they are exportable.

Examples

The following example generates a general-usage 1024-bit RSA key pair on a USB token with the label "ms2" with crypto engine debugging messages shown:

```
Router(config)# crypto key generate rsa label ms2 modulus 2048 on usbtoken0:

The name for the keys will be: ms2
% The key modulus size is 2048 bits
% Generating 1024 bit RSA keys, keys will be on-token, non-exportable...
Jan 7 02:41:40.895: crypto_engine: Generate public/private keypair [OK]
Jan 7 02:44:09.623: crypto_engine: Create signature
Jan 7 02:44:10.467: crypto_engine: Verify signature
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_CREATE_PUBKEY(hw)(ipsec)
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_PUB_DECRYPT(hw)(ipsec)
```

Now, the on-token keys labeled “ms2” may be used for enrollment.

The following example generates special-usage RSA keys:

```
Router(config)# crypto key generate rsa usage-keys

The name for the keys will be: myrouter.example.com

Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].

Choose the size of the key modulus in the range of 360 to 2048 for your Encryption Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

The following example generates general-purpose RSA keys:

Note You cannot generate both special-usage and general-purpose keys; you can generate only one or the other.

```
Router(config)# crypto key generate rsa general-keys

The name for the keys will be: myrouter.example.com

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

The following example generates the general-purpose RSA key pair “exampleCAkeys”:

```
crypto key generate rsa general-keys label exampleCAkeys
crypto ca trustpoint exampleCAkeys
 enroll url http://exampleCAkeys/certsrv/mscep/mscep.dll
 rsakeypair exampleCAkeys 1024 1024
```

The following example specifies the RSA key storage location of “usbtoken0:” for “tokenkey1”:

```
crypto key generate rsa general-keys label tokenkey1 storage usbtoken0:
```

The following example specifies the **redundancy** keyword:

```
Router(config)# crypto key generate rsa label MYKEYS redundancy

The name for the keys will be: MYKEYS
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.


How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable with redundancy...[OK]
```

Related Commands

Command	Description
copy	Copies any file from a source to a destination, use the copy command in privileged EXEC mode.
crypto key storage	Sets the default storage location for RSA key pairs.
debug crypto engine	Displays debug messages about crypto engines.
hostname	Specifies or modifies the hostname for the network server.
ip domain-name	Defines a default domain name to complete unqualified hostnames (names without a dotted-decimal domain name).
show crypto key mypubkey rsa	Displays the RSA public keys of your router.
show crypto pki certificates	Displays information about your PKI certificate, certification authority, and any registration authority certificates.

crypto key import rsa pem

To import Rivest, Shamir, and Adelman (RSA) keys in privacy-enhanced mail (PEM)-formatted files, use the **crypto key import rsa pem** command in global configuration mode.

crypto key import rsa *key-label* **pem** [**usage-keys | signature | encryption | general-purpose**] {**storage | terminal** [*passphrase*] **| url** *url*} [**exportable**] [**on** *devicename***:**]

Syntax Description

key-label	Name of the RSA key pair that is imported to the device. The *key-label* argument must match the key pair name that was specified through the **crypto key generate rsa** command.
usage-keys	(Optional) Specifies that two RSA special usage key pairs, one encryption pair and one signature pair, are imported.
signature	(Optional) Specifies that RSA signature keys are imported.
encryption	(Optional) Specifies that RSA encryption keys are imported.
general-purpose	(Optional) Specifies a General Purpose Key.
storage	Stores the key on the specified device.
terminal	Specifies the certificates and RSA key pairs are manually imported to the console terminal.
passphrase	Passphrase that is used to encrypt the PEM file for import. **Note** The passphrase can be any phrase that is at least eight characters in length; it can include spaces and punctuation, excluding the question mark (?), which has special meaning to the Cisco IOS parser.
url *url*	URL of the file system where the router should import certificates and RSA key pairs.
exportable	(Optional) Specifies that the imported RSA key pair can be exported to another Cisco device such as a router.
on *devicename***:**	(Optional) Specifies that the imported RSA key pair is created on the specified device. Devices supported include local disks, NVRAM, and USB tokens. The name of the device is followed by a colon (:). Keys created on a USB token have a maximum size of 1024-bits.

Command Default

RSA general-purpose key pair type is expected for import.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Release	Modification
12.4(11)T	This command was modified. The **signature**, **encryption**, and **on** keywords and *devicename***:** argument were added.
15.0(1)M	This command was modified. The **terminal** keyword and *passphrase* argument were added.

Usage Guidelines

The **crypto key import rsa pem** command allows RSA key pairs to be imported into PEM-formatted files. The files can be previously exported from another Cisco IOS router or generated by other public key infrastructure (PKI) applications.

As of Cisco IOS Release 12.4(11)T and later releases, the device can be specified for where RSA keys are generated. Devices supported include NVRAM, local disks and USB tokens. If the router has a USB token configured and available, the USB token can be used as cryptographic device in addition to a storage device. Using a USB token as a cryptographic device allows RSA operations such as key generation, signing and authentication of credentials to be performed on the token. The private key never leaves the USB token and is not exportable. The public key is exportable.

RSA keys may be imported to a configured and available USB token by using the **on** *devicename***:** keyword and argument. Keys that reside on a USB token, or on-token keys, are saved to persistent token storage when they are imported. Key deletion removes the on-token keys from persistent storage immediately. (Keys that do not reside on a token are saved to or deleted from nontoken storage locations when the **write memory** or similar command is issued.)

If the device, on which the RSA key is to be imported, does not have enough space for this key, then a message appears saying that the importation of the key has failed.

For information on configuring a USB token, see "Storing PKI Credentials" module. For information on using on-token RSA credentials, see "Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment" module.

Examples

The following example shows that an encryption key has been imported successfully to a configured and available USB token, shown with crypto engine and crypto PKI transaction debugging messages:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# crypto key import rsa label encryption on usbtoken0 url nvram:e password
% Importing public Encryption key or certificate PEM file...
filename [e-encr.pub]?
Reading file from nvram:e-encr.pub
% Importing private Encryption key PEM file...
Source filename [e-encr.prv]?
Reading file from nvram:e-encr.prv
% Key pair import succeeded.
```

The following example shows how to generate, export, import, and verify the status of the RSA key pair "mycs":

```
! Generate the key pair
!
Router(config)# crypto key generate rsa general-purpose label mycs exportable
The name for the keys will be: mycs
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024
```

```
% Generating 1024 bit RSA keys ...[OK]
!
! Archive the key pair to a remote location, and use a good password.
!
Router(config)# crypto key export rsa mycs pem url nvram: 3des PASSWORD
% Key name: mycs
Usage: General Purpose Key
Exporting public key...
Destination filename [mycs.pub]?
Writing file to nvram:mycs.pub
Exporting private key...
Destination filename [mycs.prv]?
Writing file to nvram:mycs.prv
!
! Import the key as a different name.
!
Router(config)# crypto key import rsa mycs2 pem url nvram:mycs PASSWORD
% Importing public key or certificate PEM file...
Source filename [mycs.pub]?
Reading file from nvram:mycs.pub
% Importing private key PEM file...
Source filename [mycs.prv]?
Reading file from nvram:mycs.prv% Key pair import succeeded.
!
! After the key has been imported, it is no longer exportable.
!
! Verify the status of the key.
!
Router# show crypto key mypubkey rsa

% Key pair was generated at: 18:04:56 GMT Jun 6 2003
Key name: mycs
Usage: General Purpose Key
Key is exportable.
Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00E65253
  9C30C12E 295AB73F B1DF9FAD 86F88192 7D4FA4D2 8BA7FB49 9045BAB9 373A31CB
  A6B1B8F4 329F2E7E 8A50997E AADBCFAA 23C29E19 C45F4F05 DBB2FA51 4B7E9F79
  A1095115 759D6BC3 5DFB5D7F BCF655BF 6317DB12 A8287795 7D8DC6A3 D31B2486
  C9C96D2C 2F70B50D 3B4CDDAE F661041A 445AE11D 002EEF08 F2A627A0 5B020301 0001
% Key pair was generated at: 18:17:25 GMT Jun 6 2003
Key name: mycs2
Usage: General Purpose Key
Key is not exportable.
Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00E65253
  9C30C12E 295AB73F B1DF9FAD 86F88192 7D4FA4D2 8BA7FB49 9045BAB9 373A31CB
  A6B1B8F4 329F2E7E 8A50997E AADBCFAA 23C29E19 C45F4F05 DBB2FA51 4B7E9F79
  A1095115 759D6BC3 5DFB5D7F BCF655BF 6317DB12 A8287795 7D8DC6A3 D31B2486
  C9C96D2C 2F70B50D 3B4CDDAE F661041A 445AE11D 002EEF08 F2A627A0 5B020301 0001
```

Related Commands

Command	Description
crypto key export pem	Exports RSA keys in PEM-formatted files.
crypto key generate rsa	Generates RSA key pairs.

crypto key lock rsa

To lock the RSA private key in a router, use the **crypto key lock rsa** command in privileged EXEC mode.

crypto key lock rsa [**name** *key-name*] [**all**] [**passphrase** [*passphrase*]]

Syntax Description

name *key-name*	(Optional) Specifies the name of the RSA key pair that is to be locked. The name must match the name that was specified via the **crypto key encrypt rsa** command.
all	(Optional) Locks all the encrypted keys.
passphrase *passphrase*	(Optional) Specifies the passphrase that is used to lock the RSA key. The passphrase must match the passphrase that was specified via the **crypto key encrypt rsa** command.

Defaults

RSA keys are encrypted, but not locked.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **all** keyword was added.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

When the **crypto key lock rsa** command is issued, the unencrypted copy of the key is deleted. Because the private key is not available, all RSA operations will fail.

This command affects only the "run-time" access to the key; that is, it does not affect the key that is stored in NVRAM.

Examples

The following example shows how to lock the key "pki1-72a.cisco.com." Thereafter, the **show crypto key mypubkey rsa** command is issued to verify that the key is protected (encrypted) and locked.

```
Router# crypto key lock rsa name pki1-72a.cisco.com passphrase cisco1234
!
Router# show crypto key mypubkey rsa

% Key pair was generated at:20:29:41 GMT Jun 20 2003
Key name:pki1-72a.cisco.com
Usage:General Purpose Key
*** The key is protected and LOCKED. ***
Key is exportable.
```

```
Key Data:
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00D7808D C5FF14AC
0D2B55AC 5D199F2F 7CB4B355 C555E07B 6D0DECBE 4519B1F0 75B12D6F 902D6E9F
B6FDAD8D 654EF851 5701D5D7 EDA047ED 9A2A619D 5639DF18 EB020301 0001
```

Related Commands

Command	Description
crypto key encrypt rsa	Encrypts the RSA private key.
crypto key unlock rsa	Unlocks the RSA private key in a router.
show crypto key mypubkey rsa	Displays the RSA public keys of your router.

crypto key move rsa

To move an existing Cisco IOS generated Rivest, Shamir, and Adelman (RSA) key pair from one storage location to another storage location, use the **crypto key move rsa** command in global configuration mode.

crypto key move rsa *keylabel* [**non-exportable**] [**on** | **storage**] [**redundancy***routername*] *location*

Syntax Description

keylabel	Specifies name of the existing RSA key pair.
non-exportable	(Optional) Specifies that the RSA key pair cannot be exported once the key pair is moved to the eToken device.
on	(Optional) Specifies that the RSA key pair will be placed on a configured USB token and stored in the PIN protected flash portion of the USB token. Any subsequent RSA operations will be performed on the USB token.
storage	(Optional) Specifies that the RSA key pair will be stored on the specified device, for example a smart card. The key pair will be loaded back into Cisco IOS for any subsequent RSA operations.
location	Identifies the storage location where the RSA key pair will be moved.
redundancy	(Optional) Specifies that the key should be synchronized to the standby CA.

Command Default

The RSA key pair remains stored on the current device.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
15.0(1)M	This command was modified. The **redundancy** keyword was introduced.

Usage Guidelines

When an existing RSA key pair is generated in Cisco IOS, stored on a USB token, and used for an enrollment, it may be necessary to move those existing RSA key pairs to an alternate location for permanent storage.

Generating the key on the router and moving it to the token requires less than a minute. Generating a key on the token using the **on** keyword could require 5 to 10 minutes and is dependent on hardware key generation routines available on the USB token.

Using the **crypto key move rsa** command allows the storage location of a newly generated key to be changed if the **storage** keyword or **on** keyword was not specified when the key was first generated and the key has not yet been written out to a storage location. You can always move an exportable key.

Note If you make the key nonexportable by issuing the **non-exportable** keyword, the key cannot be made exportable again. Also, once you specify the **on** keyword with the target device, either to move an existing key or during key generation, the command cannot be undone.

Examples

The following example moves an existing RSA key pair to a configured and available USB token, "tokenA," as a nonexportable key pair stored in the PIN protected flash portion of the designated USB token:

```
crypto key move rsa keypairname non-exportable on tokenA
```

Related Commands

Command	Description
binary file	Specifies the binary file location on the registrar and the destination binary file location on the petitioner.
template file	Specifies the source template file location on the registrar and the destination template file location on the petitioner.

crypto key pubkey-chain rsa

To enter public key configuration mode (so you can manually specify other devices' RSA public keys), use the **crypto key pubkey-chain rsa** command in global configuration mode.

crypto key pubkey-chain rsa

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to enter public key chain configuration mode. Use this command when you need to manually specify other IPSec peers' RSA public keys. You need to specify other peers' keys when you configure RSA encrypted nonces as the authentication method in an Internet Key Exchange policy at your peer router.

Examples

The following example specifies the RSA public keys of two other IPSec peers. The remote peers use their IP address as their identity.

```
Router(config)# crypto key pubkey-chain rsa
Router(config-pubkey-chain)# addressed-key 10.5.5.1
Router(config-pubkey-key)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(config-pubkey-chain)# addressed-key 10.1.1.2
Router(config-pubkey-key)# key-string
Router(config-pubkey)# 0738BC7A 2BC3E9F0 679B00FE 53987BCC
Router(config-pubkey)# 01030201 42DD06AF E228D24C 458AD228
Router(config-pubkey)# 58BB5DDD F4836401 2A2D7163 219F882E
Router(config-pubkey)# 64CE69D4 B583748A 241BED0F 6E7F2F16
Router(config-pubkey)# 0DE0986E DF02031F 4B0B0912 F68200C4
```

```
Router(config-pubkey)# C625C389 0BFF3321 A2598935 C1B1
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(config-pubkey-chain)# exit
Router(config)#
```

Related Commands

Command	Description
address	Specifies the IP address of the remote RSA public key of the remote peer you will manually configure.
addressed-key	Specifies the RSA public key of the peer you will manually configure.
key-string (IKE)	Specifies the RSA public key of a remote peer.
named-key	Specifies which peer RSA public key you will manually configure.
show crypto key pubkey-chain rsa	Displays peer RSA public keys stored on your router.

crypto key storage

To set the default storage location for newly created Rivest, Shamir, and Adelman (RSA) key pairs, use the **crypto key storage** command in global configuration mode. To store keys on the most recently logged-in USB token (or on NVRAM if there is no token), use the **no** form of this command.

crypto key storage *device*:

no crypto key storage *device*:

Syntax Description

device:	Name of the device where the RSA key pairs will be stored by default.

Command Default

RSA key pairs are stored on NVRAM.

Command Modes

Global configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.

Usage Guidelines

You may specify a default storage location, other than NVRAM, for newly created USB token RSA keys. The storage location specified by the **crypto key generate rsa** command for RSA keys will override the location specified by the **crypto key storage** command. The name of the designated device is followed by a colon (:).

Regardless of configuration settings, existing keys will be stored on the devices from where they were originally loaded.

Note The USB token must be logged into the router for the RSA keys to be read or written.

Examples

The following example shows how to store new keys in NVRAM by default, regardless of where the token is inserted:

```
crypto key storage nvram:
```

The following example shows how to store new keys on usbtoken0: by default:

```
crypto key storage usbtoken0:
```

The following example shows how to store new keys on most recently logged-in token, or on NVRAM if there is no token:

```
no crypto key storage
```

Related Commands

Command	Description
crypto key generate rsa	Generates RSA key pairs and specifies RSA key storage location (other than the default location).
crypto pki token user-pin	Creates a PIN that automatically allows the router to log into the USB token at router startup.

crypto key unlock rsa

To unlock the RSA private key in a router, use the **crypto key unlock rsa** command in privileged EXEC mode.

crypto key unlock rsa [**name** *key-name*] [**all**] [**passphrase** [*passphrase*]]

Syntax Description

name *key-name*	(Optional) Specifies the name of the RSA key pair that is to be unlocked. The name must match the name that was specified via the **crypto key encrypt rsa** command.
all	(Optional) Unlocks all the locked key pairs.
passphrase *passphrase*	(Optional) Specifies the passphrase that is used to unlock the RSA key. The passphrase must match the passphrase that was specified via the **crypto key encrypt rsa** command.

Defaults

The encrypted private key is locked.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **all** keyword was added.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

When a router with an encrypted RSA key (via the **crypto key encrypt rsa** command) initially boots up, the key does not exist in plain text and is therefore considered to be locked. Because the private key is not available, all RSA operations will fail. After you unlock the private key, RSA operations will function again.

This command affects only the “run-time” access to the key; that is, it does not affect the key that is stored in NVRAM.

Examples

The following example shows how to unlock the key “pki1-72a.cisco.com”:

```
Router# crypto key unlock rsa name pki1-72a.cisco.com passphrase cisco1234
```

Related Commands

Command	Description
crypto key encrypt rsa	Encrypts the RSA private key.
crypto key lock rsa	Locks the RSA private key in a router.
show crypto key mypubkey rsa	Displays the RSA public keys of your router.

crypto key zeroize pubkey-chain

To delete the remote peer's public key from the cache, use the **crypto key zeroize pubkey-chain** command in global configuration mode.

crypto key zeroize pubkey-chain [*index*]

Syntax Description

index	(Optional) Specifies an index entry to be deleted. If no index entry is specified, then all the index entries are deleted. The acceptable range of index entries is from 1 to 65535.

Defaults

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

This command is used is used to delete the peer router's public keys in order to help debug signature verification problems in IKEv1 and IKEv2. Keys are cached by default with the lifetime of the certificate revocation list (CRL) associated with the trustpoint.

Examples

The following example deletes all public key index entries:

```
Router# configure terminal
Router(config)# crypto key zeroize pubkey-chain
```

Related Commands

Command	Description
crypto key zeroize rsa	Deletes RSA key pairs from the router.

crypto key zeroize rsa

To delete all RSA keys from your router, use the **crypto key zeroize rsa** command in global configuration mode.

crypto key zeroize rsa [*key-pair-label*]

Syntax Description

key-pair-label	(Optional) Specifies the name of the key pair that router will delete.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(8)T	The *key-pair-label* argument was added.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command deletes all Rivest, Shamir, and Adelman (RSA) keys that were previously generated by your router unless you include the *key-pair-label* argument, which will delete only the specified RSA key pair. If you issue this command, you must also perform two additional tasks for each trustpoint that is associated with the key pair that was deleted:

- Ask the certification authority (CA) administrator to revoke your router's certificates at the CA; you must supply the challenge password you created when you originally obtained the router's certificates using the **crypto ca enroll** command.
- Manually remove the router's certificates from the configuration by removing the configured trustpoint (using the **no crypto ca trustpoint** *name* command.)

Note This command cannot be undone (after you save your configuration), and after RSA keys have been deleted, you cannot use certificates or the CA or participate in certificate exchanges with other IP Security (IPSec) peers unless you reconfigure CA interoperability by regenerating RSA keys, getting the CA's certificate, and requesting your own certificate again.

This command is not saved to the configuration.

Examples

The following example deletes the general-purpose RSA key pair that was previously generated for the router. After deleting the RSA key pair, the administrator contacts the CA administrator and requests that the certificate of the router be revoked. The administrator then deletes the certificate of the router from the configuration.

```
crypto key zeroize rsa
crypto ca certificate chain
 no certificate
```

Related Commands

Command	Description
certificate	Adds certificates manually.
crypto ca certificate chain	Enters the certificate chain configuration mode.
crypto ca trustpoint	Declares the CA that your router should use.
show crypto ca timers	Specifies which key pair to associate with the certificate.

crypto keyring

To define a crypto keyring to be used during Internet Key Exchange (IKE) authentication, use the **crypto keyring** command in global configuration mode. To remove the keyring, use the **no** form of this command.

crypto keyring *keyring-name* [**vrf** *fvrf-name*]

no crypto keyring *keyring-name* [**vrf** *fvrf-name*]

Syntax Description

keyring-name	Name of the crypto keyring.
vrf *fvrf-name*	(Optional) Front door virtual routing and forwarding (FVRF) name to which the keyring will be referenced. The *fvrf-name* must match the FVRF name that was defined during virtual routing and forwarding (VRF) configuration. The **vrf** keyword and *fvrf-name* argument are not supported by IPv6.

Command Default

All the Internet Security Association and Key Management Protocol (ISAKMP) keys that were defined in the global configuration are part of the default global keyring.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(4)T	Support for IPv6 was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

A keyring is a repository of preshared and Rivest, Shamir, and Adelman (RSA) public keys. The keyring is used in the ISAKMP profile configuration mode. The ISAKMP profile successfully completes authentication of peers if the peer keys are defined in the keyring that is attached to this profile.

Examples

The following example shows that a keyring and its usage have been defined:

```
crypto keyring vpnkeys
  pre-shared-key address 10.72.23.11 key vpnsecret
crypto isakmp profile vpnprofile
  keyring vpnkeys
```

Related Commands

Command	Description
pre-shared-key	Defines a preshared key to be used for IKE authentication.

crypto logging ezvpn

To enable Easy VPN syslog messages on a server, use the **crypto logging ezvpn** command in global configuration mode. To disable syslog messages on the server, use the **no** form of this command.

crypto logging ezvpn [**group** *group-name*]

no crypto logging ezvpn [**group** *group-name*]

Syntax Description

group *group-name*	(Optional) Group name. If a group name is not provided, syslog messages are enabled for all Easy VPN connections to the server. If a group name is provided, syslog messages are enabled only for that particular group.

Command Default

Syslog messages are not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Examples

The following configuration shows that syslog messages are to be displayed for group_1.

```
crypto logging ezvpn group group_1
```

The following is an example of a typical Easy VPN syslog message:

```
timestamp: %CRYPTO-6-VPN_TUNNEL_STATUS: (Server)  <event message>  User=<username>
Group=<groupname>  Client_public_addr=<ip_addr> Server_public_addr=<ip addr>
```

The following is an example of an authentication-passed event Easy VPN syslog message:

```
Jul 25 23:33:06.847: %CRYPTO-6-VPN_TUNNEL_STATUS: (Server)  Authentication PASS
ED  User=blue Group=Cisco1760group  Client_public_addr=10.20.20.1
Server_public_addr=10.20.20.2
```

The following is an example of a “Group does not exist” Easy VPN syslog message:

```
*Jun 30 18:02:58.107: %CRYPTO-6-VPN_TUNNEL_STATUS: Group: group_1 does not exist
```

crypto logging ikev2

To enable Internet Key Exchange Version 2 (IKEv2) syslog messages, use the **crypto logging ikev2** command in global configuration mode. To disable syslog messages, use the **no** form of this command.

crypto logging ikev2

no crypto logging ikev2

Syntax Description

This command has no keywords or arguments.

Command Default

IKEv2 syslog messages are not enabled.

Command Modes

Global configuration (config)

Command Historyb

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Examples

The following configuration shows how to enable IKEv2 syslog messages:

```
Router(config)# crypto logging ikev2
```

Related Commands

Command	Description
crypto ikev2 certificate-cache	Specifies the cache size to store certificates fetched from HTTP URLs.
crypto ikev2 cookie-challenge	Enables IKEv2 cookie challenge.
crypto ikev2 diagnose error	Enables IKEv2 error diagnosis.
crypto ikev2 dpd	Defines DPD globally for all peers.
crypto ikev2 http-url cert	Enables HTTP CERT support.
crypto ikev2 limit	Defines call admission control for all peers.
crypto ikev2 nat	Defines NAT keepalive globally for all peers.
crypto ikev2 window	Specifies the IKEv2 window size.

crypto logging session

To generate crypto logging messages, use the **crypto logging session** command in global configuration mode. To disable logging messages, use the **no** form of this command.

crypto logging session

no crypto logging session

Syntax Description

session	Generates the log of active or up sessions, and inactive or down sessions.

Command Default

Crypto logging messages are not generated.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

Crypto logging messages allow users to receive notification for every crypto EZVPN group or session that is made on their device.

Examples

The following example shows how to enable crypto logging syslog messages for all the sessions:

```
Router(config)# crypto logging session
```

Related Commands

Command	Description
crypto logging ezvpn	Enables Easy VPN syslog messages on a server.
show logging	Displays the state of system logging and the contents of the standard system logging buffer.

crypto map (global IPsec)

To enter crypto map configuration mode and create or modify a crypto map entry, to create a crypto profile that provides a template for configuration of dynamically created crypto maps, or to configure a client accounting list, use the **crypto map** command in global configuration mode. To delete a crypto map entry, profile, or set, use the **no** form of this command.

crypto map [**ipv6**] *map-name seq-num* [**ipsec-manual**]

crypto map [**ipv6**] *map-name seq-num* [**ipsec-isakmp** [**dynamic** *dynamic-map-name* | **discover** | **profile** *profile-name*]]

no crypto map [**ipv6**] *map-name* [*seq-num*]

crypto map [**ipv6**] *map-name* **client accounting list** *aaalist*

no crypto map [**ipv6**] *map-name* [**client accounting list**]

crypto map *map-name seq num* [**gdoi**]

no crypto map *map-name* [*seq-num*]

Syntax Description

ipv6	(Optional) Specifies an IPv6 crypto map. For IPv4 crypto maps, use the command without this keyword. **Note** IPv6 addresses are not supported on dynamic crypto maps.
map-name	Identifies the crypto map set.
seq-num	Sequence number you assign to the crypto map entry. See additional explanation for using this argument in the "Usage Guidelines" section.
ipsec-manual	(Optional) Indicates that Internet Key Exchange (IKE) will not be used to establish the IP Security (IPsec) security associations (SAs) for protecting the traffic specified by this crypto map entry. **Note** The **ipsec-manual** keyword is not supported by the virtual private network Shared Port Adapter (VPN SPA) beginning with Cisco IOS Release 12.2(33)SXH5 or 12.2(33)SXI1. If the **ipsec-manual** keyword is entered for images after those releases, the following error message appears beneath the keyword entry line: "Manually-keyed crypto map configuration is not supported by the current crypto engine."
ipsec-isakmp	(Optional) Indicates that IKE will be used to establish the IPsec for protecting the traffic specified by this crypto map entry.
dynamic	(Optional) Specifies that this crypto map entry must reference a preexisting dynamic crypto map. **Note** Dynamic crypto maps are policy templates used in processing negotiation requests from a peer IPsec device. If you use this keyword, none of the crypto map configuration commands will be available.
dynamic-map-name	(Optional) Name of the dynamic crypto map set that should be used as the policy template.
discover	(Optional) Enables peer discovery. By default, peer discovery is disabled.

profile	(Optional) Designates a crypto map as a configuration template. The security configurations of this crypto map will be cloned as new crypto maps are created dynamically on demand.
profile-name	(Optional) Name of the crypto profile being created.
client accounting list	Designates a client accounting list.
aaalist	(Optional) AAA list name.
gdoi	(Optional) Indicates that the key management mechanism is Group Domain of Interpretation (GDOI).

Command Default

No crypto maps exist.
Peer discovery is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
11.3T	The following keywords and arguments were added: • **ipsec-manual** • **ipsec-isakmp** • **dynamic** • *dynamic-map-name*
12.0(5)T	The **discover** keyword was added to support Tunnel Endpoint Discovery (TED).
12.2(4)T	The **profile** *profile-name* keyword-argument pair was added to allow the generation of a crypto map profile that is cloned to create dynamically created crypto maps on demand.
12.2(11)T	This command was implemented on the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.
12.2(15)T	The **client accounting list** *aaalist* keyword-argument pair was added.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB without support for the **gdoi** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH5, 12.2(33)SXI1	The **ipsec-manual** keyword is not supported by the VPN SPA beginning with Cisco IOS Release 12.2(33)SXH5 or 12.2(33)SXI1.
12.4(6)T	The **gdoi** keyword was added.
Cisco IOS XE 2.1	This command was implemented on Cisco ASR 1000 series routers.
15.1(4) M	This command was modified. The **ipv6** keyword was added.

Usage Guidelines

Use this command to create a new crypto map entry or profile. Use the **crypto map ipv6** *map-name seq-num* command without any keyword to modify an existing IPv6 crypto map entry or profile. For IPv4 crypto maps, use the **crypto map** *map-name seq-num* command without any keyword to modify the existing crypto map entry or profile.

After a crypto map entry is created, you cannot change the parameters specified at the global configuration level because these parameters determine the configuration commands that are valid at the crypto map level. For example, after a map entry has been created using the **ipsec-isakmp** keyword, you cannot change it to the option specified by the **ipsec-manual** keyword; you must delete and reenter the map entry.

After you define crypto map entries, you can assign the crypto map set to interfaces using the **crypto map** (interface IPsec) command.

Crypto Map Functions

Crypto maps provide two functions: filtering and classifying the traffic to be protected and defining the policy to be applied to that traffic. The first affects the flow of traffic on an interface; the second affects the negotiation performed (via IKE) on behalf of that traffic.

IPsec crypto maps define the following:

- What traffic should be protected
- To which IPsec peers the protected traffic can be forwarded—these are the peers with which an SA can be established
- Which transform sets are acceptable for use with the protected traffic
- How keys and SAs should be used or managed (or what the keys are, if IKE is not used)

Multiple Crypto Map Entries with the Same Map Name Form a Crypto Map Set

A crypto map set is a collection of crypto map entries, each with a different *seq-num* argument but the same *map-name* argument. Therefore, for an interface, you could have certain traffic forwarded to one IPsec peer with specified security applied to that traffic and other traffic forwarded to the same or different IPsec peer with different IPsec security applied. To accomplish differential forwarding, you would create two crypto maps, each with the same *map-name* argument but different *seq-num* argument. Crypto profiles must have unique names within a crypto map set.

Note If a deny statement (which specifies the conditions under which a packet cannot pass the access control list) in an access control list belongs to a crypto map in a crypto map set, the IPsec logic causes a jump to the next crypto map in the crypto map set, hoping for a better possible match. VPN Service Adapter (VSA) hardware has a restriction of 14 jumps.

Sequence Numbers

The number you assign to the *seq-num* argument should not be arbitrary. This number is used to rank multiple crypto map entries within a crypto map set. Within a crypto map set, a crypto map entry with a lower *seq-num* is evaluated before a map entry with a higher *seq-num*; that is, the map entry with the lower number has a higher priority.

For example, assume that a crypto map set contains three crypto map entries: mymap 10, mymap 20, and mymap 30. The crypto map set named "mymap" is applied to serial interface 0. When traffic passes through serial interface 0, traffic is evaluated first for mymap 10. If the traffic matches any access list permit statement entry in the extended access list in mymap 10, the traffic will be processed according to the information defined in mymap 10 (which includes establishing IPsec SAs when necessary). If the

traffic does not match the mymap 10 access list, the traffic will be evaluated for mymap 20, and then mymap 30, until the traffic matches a permit entry in a map entry. (If the traffic does not match a permit entry in any crypto map entry, it will be forwarded without any IPsec security.)

Dynamic Crypto Maps

Refer to the "Usage Guidelines" section of the **crypto dynamic-map** command for a discussion on dynamic crypto maps.

Crypto map entries that reference dynamic map sets should be the lowest priority map entries, allowing inbound SA negotiation requests to try to match the static maps first. If the request does not match any of the static maps, it will be evaluated against the dynamic map set.

If a crypto map entry references a dynamic crypto map set, make it the lowest priority map entry by giving it the highest *seq-num* value of all the map entries in a crypto map set.

Create dynamic crypto map entries using the **crypto dynamic-map** command. After you create a dynamic crypto map set, add the dynamic crypto map set to a static crypto map set with the **crypto map** (global IPsec) command using the **dynamic** keyword.

Note IPv6 keywords are not supported on dynamic crypto maps.

TED

Tunnel Endpoint Discovery (TED) is an enhancement to the IPsec feature. Defining a dynamic crypto map allows you to dynamically determine an IPsec peer; however, only the receiving router has this ability. With TED, the initiating router can dynamically determine an IPsec peer for secure IPsec communications.

Dynamic TED helps to simplify the IPsec configuration on individual routers within a large network. Each node has a simple configuration that defines the local network that the router is protecting and the IPsec transforms that are required.

Note TED helps only in discovering peers; otherwise, TED does not function any differently from normal IPsec. Thus, TED does not improve the scalability of IPsec (in terms of performance or the number of peers or tunnels).

Crypto Map Profiles

Crypto map profiles are created using the **profile** *profile-name* keyword and argument combination. Crypto map profiles are used as configuration templates for dynamically creating crypto maps on demand for use with the L2TP Security feature. The relevant SAs in the crypto map profile will be cloned and used to protect IP traffic on the L2TP tunnel.

Note The **set peer** and **match address** commands are ignored by crypto profiles and should not be configured in the crypto map definition.

Examples

The following example shows the minimum required crypto map configuration when IKE will be used to establish the SAs:

```
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
```

```
 set peer 10.0.0.1
```

The following example shows the minimum required IPv6 crypto map configuration when IKE will be used to establish the SAs:

```
crypto map ipv6 CM_V6 10 ipsec-isakmp
 match address ACL_IPV6_1
  set peer 2001:DB8:0:ABCD::1
```

The following example shows the minimum required crypto map configuration when the SAs are manually established:

```
crypto transform-set someset ah-md5-hmac esp-des
crypto map mymap 10 ipsec-manual
 match address 102
 set transform-set someset
 set peer 10.0.0.5
 set session-key inbound ah 256 98765432109876549876543210987654
 set session-key outbound ah 256 fedcbafedcbafedcfedcbafedcbafedc
 set session-key inbound esp 256 cipher 0123456789012345
 set session-key outbound esp 256 cipher abcdefabcdefabcd
```

The following example shows the minimum required IPv6 crypto map configuration when the SAs are manually established:

```
crypto map ipv6 CM_V6 ipsec-manual
 match address ACL_V6_2
 set transform-set someset
 set peer 2001:DB8:0:ABCD::1
 set session-key inbound ah 256 98765432109876549876543210987654
 set session-key outbound ah 256 fedcbafedcbafedcfedcbafedcbafedc
 set session-key inbound esp 256 cipher 0123456789012345
 set session-key outbound esp 256 cipher abcdefabcdefabcd
```

The following example shows how to configure an IPsec crypto map set that includes a reference to a dynamic crypto map set.

Crypto map “mymap 10” allows SAs to be established between the router and either or both the remote IPsec peers for traffic matching access list 101. Crypto map “mymap 20” allows either of the two transform sets to be negotiated with the remote peer for traffic matching access list 102.

Crypto map entry “mymap 30” references the dynamic crypto map set “mydynamicmap,” which can be used to process inbound SA negotiation requests that do not match “mymap” entries 10 or 20. In this case, if the peer specifies a transform set that matches one of the transform sets specified in “mydynamicmap,” for a flow permitted by the access list 103, IPsec will accept the request and set up SAs with the remote peer without previously knowing about the remote peer. If the request is accepted, the resulting SAs (and temporary crypto map entry) are established according to the settings specified by the remote peer.

The access list associated with “mydynamicmap 10” is also used as a filter. Inbound packets that match any access list permit statement in this list are dropped for not being IPsec protected. (The same is true for access lists associated with static crypto maps entries.) Outbound packets that match a permit statement without an existing corresponding IPsec SA are also dropped.

```
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
 set peer 10.0.0.2
crypto map mymap 20 ipsec-isakmp
 match address 102
 set transform-set my_t_set1 my_t_set2
```

```
 set peer 10.0.0.3
crypto map mymap 30 ipsec-isakmp dynamic mydynamicmap
!
crypto dynamic-map mydynamicmap 10
 match address 103
 set transform-set my_t_set1 my_t_set2 my_t_set3
```

The following example shows how to configure TED on a Cisco router:

```
crypto map testtag 10 ipsec-isakmp dynamic dmap discover
```

The following example shows how to configure a crypto profile to be used as a template for dynamically created crypto maps when IPsec is used to protect an L2TP tunnel:

```
crypto map l2tpsec 10 ipsec-isakmp profile l2tp
```

The following example shows how to configure a crypto map for a GDOI group member:

```
crypto map diffint 10 gdoi
 set group diffint
```

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters crypto map configuration command mode.
crypto isakmp profile	Audits IPsec user sessions.
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPsec traffic.
match address (IPSec)	Specifies an extended access list for a crypto map entry.
set peer (IPsec)	Specifies an IPsec peer in a crypto map entry.
set pfs	Specifies that IPsec should ask for PFS when requesting new SAs for this crypto map entry, or that IPsec requires PFS when receiving requests for new SAs.
set session-key	Specifies the IPsec session keys within a crypto map entry.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPsec)	Displays the crypto map configuration.

crypto map (interface IPsec)

To apply a previously defined crypto map set to an interface, use the **crypto map** command in interface configuration mode. To remove the crypto map set from the interface, use the **no** form of this command.

crypto map *map-name* [**redundancy** *standby-group-name* [**stateful**]]

no crypto map [*map-name*] [**redundancy** *standby-group-name* [**stateful**]]

Syntax Description

map-name	Name that identifies the crypto map set. This is the name assigned when the crypto map was created. When the **no** form of the command is used, this argument is optional. Any value supplied for the argument is ignored.
redundancy	(Optional) Defines a backup IP security (IPsec) peer. Both routers in the standby group are defined by the redundancy *standby-group-name* argument and share the same virtual IP address.
standby-group-name	(Optional) Refers to the name of the standby group as defined by Hot Standby Router Protocol (HSRP) standby commands.
stateful	(Optional) Enables IPsec stateful failover for the crypto map.

Defaults

No crypto maps are assigned to interfaces.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.2	This command was introduced.
12.1(9)E	This command was modified. The **redundancy** keyword and *standby-group-name* argument were added.
12.2(8)T	This command was modified. The **redundancy** keyword and *standby-group-name* argument were added.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5800 platforms.
12.2(9)YE	This command was modified. The **redundancy** keyword and *standby-group-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(11)T	This command was modified. The **stateful** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to assign a crypto map set to an interface. You must assign a crypto map set to an interface before that interface can provide IPsec services. Only one crypto map set can be assigned to an interface. If multiple crypto map entries have the same map name but a different sequence number, they are considered to be part of the same set and will all be applied to the interface. The crypto map entry that has the lowest sequence number is considered the highest priority and will be evaluated first. A single crypto map set can contain a combination of **ipsec-isakmp** and **ipsec-manual crypto map** entries.

Note A crypto map applied to a loopback interface is not supported.

The standby name must be configured on all devices in the standby group, and the standby address must be configured on at least one member of the group. If the standby name is removed from the router, the IPSec security associations (SAs) will be deleted. If the standby name is added again, regardless of whether the same name or a different name is used, the crypto map (using the **redundancy** option) will have to be reapplied to the interface.

Note A virtual IP address must be configured in the standby group to enable either stateless or stateful redundancy.

The **stateful** keyword enables stateful failover of The Internet Key Exchange (IKE) and IPsec sessions. Stateful Switchover (SSO) must also be configured for IPsec stateful failover to operate correctly.

Note A crypto map cannot be applied to a tunnel interface. If you try to apply the tunnel interface to a crypto map, an error message is displayed as follows: `crypto map is configured on tunnel interface. Currently only Group Domain of Interpretation (GDOI) crypto map is supported on tunnel interface`.

Examples

The following example shows how to connect all remote Virtual Private Network (VPN) gateways to the router via 192.168.0.3::

```
crypto map mymap 1 ipsec-isakmp
 set peer 10.1.1.1
 reverse-route
 set transform-set esp-3des-sha
 match address 102

Interface FastEthernet 0/0
 ip address 192.168.0.2 255.255.255.0
 standby name group1
 standby ip 192.168.0.3
 crypto map mymap redundancy group1

access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
```

The crypto map on the interface binds this standby address as the local tunnel endpoint for all instances of mymap and, at the same time, ensures that stateless HSRP failover is facilitated between an active and standby device that belongs to the same standby group, named group1.

Reverse route injection (RRI) is also enabled to provide the ability for only the *active* device in the HSRP group to be advertising itself to inside devices as the next hop VPN gateway to the remote proxies. If a failover occurs, routes are deleted on the former active device and created on the new active device.

The following example shows how to configure IPSec stateful failover on the crypto map named to-per-outside:

```
crypto map to-peer-outside 10 ipsec-isakmp
 set peer 209.165.200.225
 set transform-set trans1
 match address peer-outside

interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 preempt
 standby 1 name HA-out
 standby 1 track Ethernet1/0
 crypto map to-peer-outside redundancy HA-out stateful
```

Related Commands

Command	Description
crypto map (global IPsec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPsec traffic.
redundancy inter-device	Configures redundancy and enters inter-device configuration mode.
show crypto map (IPsec)	Displays the crypto map configuration.
standby ip	Assigns an IP address that is to be shared among the members of the HSRP group and owned by the primary IP address.
standby name	Assigns a user-defined group name to the HSRP redundancy group.

crypto map (Xauth)

To configure Internet Key Exchange (IKE) extended authentication (Xauth) on a router, use the **crypto map** command in global configuration mode. To restore the default value, use the **no** form of this command.

crypto map [**ipv6**] *map-name* **client authentication list** *list-name*

no crypto map [**ipv6**] *map-name* [**client authentication list**]

Syntax Description

ipv6	(Optional) Specifies an IPv6 crypto map. For IPv4 crypto maps, use the command without this keyword.
map-name	Name you assign to the crypto map set.
client authentication list	Designates an extended user authentication method.
list-name	Character string used to name the list of authentication methods activated when a user logs in. The list name must match the list name defined during AAA configuration.

Defaults

Xauth is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(4)M	This command was modified. The **ipv6** keyword was added.

Usage Guidelines

Before configuring Xauth, you should complete the following tasks:

- Set up an authentication list using AAA commands.
- Configure an IP Security transform.
- Configure a crypto map.
- Configure Internet Security Association Key Management Protocol (ISAKMP) policy.

After enabling Xauth, you should apply the crypto map on which Xauth is configured to the router interface.

Examples

The following example shows how to configure user authentication (a list of authentication methods called *xauthlist*) on an existing static crypto map called *xauthmap*:

```
crypto map xauthmap client authentication list xauthlist
```

The following example shows how to configure user authentication (a list of authentication methods called *CM_V6list)* on an existing static IPv6 crypto map called *CM_V6*:

```
crypto map ipv6 CM_V6 client authentication list CM_V6list
```

The following example shows how to configure user authentication (a list of authentication methods called *xauthlist*) on a dynamic crypto map called *xauthdynamic* that has been applied to a static crypto map called *xauthmap*:

```
crypto map xauthmap client authentication list xauthlist
crypto map xauthmap 10 ipsec-isakmp dynamic xauthdynamic
```

Related Commands

Command	Description
aaa authentication login	Sets AAA authentication at login.
crypto ipsec transform-set	Defines a transform set, which is an acceptable combination of security protocols and algorithms, and enters crypto transform configuration mode.
crypto isakmp key	Configures a preshared authentication key.
crypto isakmp policy	Defines an IKE policy, and enters ISAKMP policy configuration mode.
crypto map (global configuration)	Creates or modifies a crypto map entry, and enters the crypto map configuration mode.
interface	Enters the interface configuration mode.

crypto map client configuration address

To configure IKE Mode Configuration on your router, use the **crypto map client configuration address** command in global configuration mode. To disable IKE Mode Configuration, use the **no** form of this command.

crypto map *tag* **client configuration address** [**initiate** | **respond**]

no crypto map *tag* **client configuration address**

Syntax Description

tag	The name that identifies the crypto map.
initiate	(Optional) A keyword that indicates the router will attempt to set IP addresses for each peer.
respond	(Optional) A keyword that indicates the router will accept requests for IP addresses from any requesting peer.

Defaults

IKE Mode Configuration is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XE	This command was introduced.
12.0(7)T	This command was implemented in Cisco IOS release 12.0(7)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

At the time of this publication, this feature is an IETF draft with limited support. Therefore this feature was not designed to enable the configuration mode for every IKE connection by default.

Examples

The following examples configure IKE Mode Configuration on your router:

```
crypto map dyn client configuration address initiate
crypto map dyn client configuration address respond
```

Related Commands

Command	Description
crypto map (global)	Creates or modifies a crypto map entry and enters the crypto map configuration mode

crypto map gdoi fail-close

To specify that the crypto map is to work in fail-close mode, use the **crypto map gdoi fail-close** command in global configuration mode. To disable fail-close mode, use the no form of this command.

crypto map *map-number* **gdoi fail-close**

no crypto map *map-number* **gdoi fail-close**

Syntax Description

This command has no arguments or keywords.

Command Default

Crypto map is not in fail-close mode.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Examples

The following example shows that fail-close mode has been activated, and unencrypted traffic from access list 102 is allowed before the group member is registered:

```
crypto map map1 gdoi fail-close
 match address 102
 activate
crypto map map1 10 gdoi
 set group ks1_group
 match address 101
!
access-list 101 deny ip 10.0.1.0 0.0.0.255 10.0.1.0 0.0.0.255
access-list 102 deny tcp any eq telnet any
```

crypto map (isakmp)

To enable Internet Key Exchange (IKE) querying of authentication, authorization, and accounting (AAA) for tunnel attributes in aggressive mode, use the **crypto map** command in global configuration mode. To restore the default value, use the **no** form of this command.

crypto map [**ipv6**] *map-name* **isakmp authorization list** *list-name*

no crypto map [**ipv6**] *map-name* [**isakmp authorization list**]

Syntax Description

ipv6	(Optional) Specifies an IPv6 crypto map. For IPv4 crypto maps, use the command without this keyword.
map-name	Name you assign to the crypto map set.
isakmp authorization list	Specifies the Internet Security Association Key Management Protocol (ISAKMP) configuration settings and authorization parameters.
list-name	Character string used to name the list of authorization methods activated when a user logs in. The list name must match the list name defined during AAA configuration.

Defaults

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(4)M	This command was modified. The **ipv6** keyword was added.

Usage Guidelines

Use this command to enable key lookup from an AAA server.

Preshared keys deployed in a large-scale Virtual Private Network (VPN) without a certification authority, with dynamic IP addresses, are accessed during aggression mode of IKE negotiation through an AAA server. Thus, users have their own key, which is stored on an external AAA server. This allows for the central management of the user database, linking it to an existing database and allowing all users to have their own unique and secure pre-shared keys.

Before configuring this command, you should perform the following tasks:

- Set up an authorization list using AAA commands.
- Configure an IPsec transform.
- Configure a crypto map.

- Configure an ISAKMP policy using IPsec and IKE commands.

After enabling this command, you should apply the previously defined crypto map to the interface.

Examples

The following example shows how to configure the **crypto map** command for IPv4 crypto maps:

```
crypto map ikessaaamap isakmp authorization list ikessaaalist
crypto map ikessaaamap 10 ipsec-isakmp dynamic ikessaaadyn
```

The following example shows how to configure the **crypto map** command for IPv6 crypto maps:

```
crypto map ipv6 CM_V6 isakmp authorization list aaa
crypto map ipv6 CM_V6 10 ipsec-isakmp dynamic aaadyn
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict a user's network access.
crypto ipsec transform-set	Defines a transform set, which is an acceptable combination of security protocols and algorithms, and enters crypto transform configuration mode.
crypto isakmp key	Configures a preshared authentication key.
crypto isakmp policy	Defines an IKE policy and enters ISAKMP policy configuration mode.
crypto map (global configuration)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
interface	Enters interface configuration mode.

crypto map isakmp-profile

To configure an Internet Security Association and Key Management Protocol (ISAKMP) profile on a crypto map, use the **crypto map isakmp-profile** command in global configuration mode. To restore the default values on the crypto map, use the **no** form of this command.

crypto map *map-name* **isakmp-profile** *isakmp-profile-name*

no crypto map *map-name* **isakmp-profile** *isakmp-profile-name*

Syntax Description

map-name	Name assigned to the crypto map set.
isakmp-profile-name	Character string used to name the ISAKMP profile that is used during an Internet Key Exchange (IKE) Phase 1 and Phase 1.5 exchange. The *isakmp-profile-name* must match the ISAKMP profile name that was defined during the ISAKMP profile configuration.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

This command describes the ISAKMP profile to use to start the IKE exchange. Before configuring this command, you must set up the ISAKMP profile.

Examples

The following example shows that an ISAKMP profile is configured on a crypto map:

```
crypto map vpnmap isakmp-profile vpnprofile
```

Related Commands

Command	Description
crypto ipsec transform-set	Defines a transform set—an acceptable combination of security protocols and algorithms.
crypto map (global)	Creates or modifies a crypto map entry.

crypto map local-address

To specify and name an identifying interface to be used by the crypto map for IPSec traffic, use the **crypto map local-address** command in global configuration mode. To remove this command from the configuration, use the **no** form of this command.

crypto map *map-name* **local-address** *interface-id*

no crypto map *map-name* **local-address**

Syntax Description

map-name	Name that identifies the crypto map set. This is the name assigned when the crypto map was created.
interface-id	The identifying interface that should be used by the router to identify itself to remote peers. If Internet Key Exchange is enabled and you are using a certification authority (CA) to obtain certificates, this should be the interface with the address specified in the CA certificates.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you apply the same crypto map to two interfaces and do not use this command, two separate security associations (with different local IP addresses) could be established to the same peer for similar traffic. If you are using the second interface as redundant to the first interface, it could be preferable to have a single security association (with a single local IP address) created for traffic sharing the two interfaces. Having a single security association decreases overhead and makes administration simpler.

This command allows a peer to establish a single security association (and use a single local IP address) that is shared by the two redundant interfaces.

If applying the same crypto map set to more than one interface, the default behavior is as follows:

- Each interface will have its own security association database.
- The IP address of the local interface will be used as the local address for IPSec traffic originating from/destined to that interface.

However, if you use a local-address for that crypto map set, it has multiple effects:

- Only one IPSec security association database will be established and shared for traffic through both interfaces.
- The IP address of the specified interface will be used as the local address for IPSec (and IKE) traffic originating from or destined to that interface.

One suggestion is to use a loopback interface as the referenced local address interface, because the loopback interface never goes down.

Examples

The following example assigns crypto map set "mymap" to the S0 interface and to the S1 interface. When traffic passes through either S0 or S1, the traffic will be evaluated against the all the crypto maps in the "mymap" set. When traffic through either interface matches an access list in one of the "mymap" crypto maps, a security association will be established. This same security association will then apply to both S0 and S1 traffic that matches the originally matched IPSec access list. The local address that IPSec will use on both interfaces will be the IP address of interface loopback0.

```
interface S0
 crypto map mymap

interface S1
 crypto map mymap

crypto map mymap local-address loopback0
```

Related Commands

Command	Description
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.

crypto map redundancy replay-interval

To modify the interval at which inbound and outbound replay updates are passed from an active device to a standby device, use the **crypto map redundancy replay-interval** command in global configuration mode. To return to the default functionality, use the **no** form of this command.

crypto map *map-name* **redundancy replay-interval inbound** *in-value* **outbound** *out-value*

no crypto map *map-name* **redundancy replay-interval inbound** *in-value* **outbound** *out-value*

Syntax Description

map-name	Name that identifies the crypto map set. This is the name assigned when the crypto map was created.
inbound *in-value*	Number of inbound packets that are processed before an anti-replay update is sent from the active router to the standby router.
outbound *out-value*	Number of outbound packets that are processed before an anti-replay update is sent from the active router to the standby router.

Defaults

inbound *in-value*: one update every 1,000 packets

outbound *out-value*: one update every 100,000 packets

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

Note This command can be used only in conjunction with IPSec stateful failover on a crypto map.

Stateful failover enables a router to continue processing and forwarding packets after a planned or unplanned outage occurs; that is, a backup (secondary) router automatically takes over the tasks of the active (primary) router if the active router loses connectivity for any reason.

The **crypto map redundancy replay-interval** command allows you to modify the interval in which an IP redundancy-enabled crypto map sends anti-replay updates from the active router to the standby router.

Examples

The following example shows how to enable replay checking for the crypto map “to-peer-outside” and enable IPSec stateful failover:

```
crypto map to-peer-outside redundancy replay-interval inbound 1000 outbound 10000
crypto map to-peer-outside 10 ipsec-isakmp
 set peer 209.165.200.225
 set transform-set trans1
```

```
 match address peer-outside
!
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 preempt
 standby 1 name HA-out
 standby 1 track Ethernet1/0
 crypto map to-peer-outside redundancy HA-out stateful
```

crypto mib ipsec flowmib history failure size

To change the size of the IP Security (IPSec) MIB failure history table, use the **crypto mib ipsec flowmib history failure size** command in global configuration mode.

crypto mib ipsec flowmib history failure size *number*

Syntax Description

number	Size of the failure history table.

Defaults

If this command is not used, the default table size is 200.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)E	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **crypto mib ipsec flowmib history failure size** command to change the size of a failure history table. If you do not configure the size of a failure history table, the default of 200 will be implemented.

A failure history table stores the reason for tunnel failure and the time failure occurred. A failure history table can be used as a simple method to distinguish between a normal and an abnormal tunnel termination. That is, if a tunnel entry in the tunnel history table has no associated failure record, the tunnel must have terminated normally. However, every failure does not correspond to a tunnel. Supported setup failures are recorded in the failure table, but a history table is not associated because a tunnel was never set up.

Examples

The following example shows the size of a failure history table configured to be 140:

```
crypto mib ipsec flowmib history failure size 140
```

Related Commands

Command	Description
crypto mib ipsec flowmib history tunnel size	Changes the size of the IPSec tunnel history table.
show crypto mib ipsec flowmib history failure size	Displays the size of the IPSec failure history table.

crypto mib ipsec flowmib history tunnel size

To change the size of the IP Security (IPSec) tunnel history table, use the **crypto mib ipsec flowmib history tunnel size** command in global configuration mode.

crypto mib ipsec flowmib history tunnel size *number*

Syntax Description

number	Size of the tunnel history table.

Defaults

The default table size is 200.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)E	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **crypto mib ipsec flowmib history tunnel size** command to change the size of a tunnel history table. If you do not configure the size of a tunnel history table, the default of 200 will be implemented.

A tunnel history table stores the attribute and statistics records, which contain the attributes and the last snapshot of the traffic statistics of a given tunnel. A tunnel history table accompanies a failure table, so you can display the complete history of a given tunnel. However, a tunnel history table does not accompany every failure table because every failure does not correspond to a tunnel. Thus, supported setup failures are recorded in the failure table, but an associated history table is not recorded because a tunnel was never set up.

As an optimization, a tunnel endpoint table can be combined with a tunnel history table. However, if a tunnel endpoint table is combined, all three tables (the failure history table, tunnel history table, and the endpoint table) must remain the same size even though the MIB allows each table to be distinct.

Examples

The following example shows the size of a tunnel history table configured to be 130:

```
crypto mib ipsec flowmib history tunnel size 130
```

Related Commands

Command	Description
crypto mib ipsec flowmib history failure size	Changes the size of the IPSec failure history table.
show crypto mib ipsec flowmib history tunnel size	Displays the size of the IPSec tunnel history table.

crypto pki authenticate

To authenticate the certification authority (CA) (by getting the certificate of the CA), use the **crypto pki authenticate** command in global configuration mode.

crypto pki authenticate *name*

Syntax Description

name	The name of the CA. This is the same name used when the CA was declared with the **crypto ca identity** command.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3T	The **crypto ca authenticate** command was introduced.
12.3(7)T	This command replaced the **crypto ca authenticate** command.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

This command is required when you initially configure CA support at your router.

This command authenticates the CA to your router by obtaining the self-signed certificate of the CA that contains the public key of the CA. Because the CA signs its own certificate, you should manually authenticate the public key of the CA by contacting the CA administrator when you enter this command.

If you are using Router Advertisements (RA) mode (using the **enrollment** command) when you issue the **crypto pki authenticate** command, then registration authority signing and encryption certificates will be returned from the CA and the CA certificate.

This command is not saved to the router configuration. However. the public keys embedded in the received CA (and RA) certificates are saved to the configuration as part of the Rivest, Shamir, and Adelman (RSA) public key record (called the "RSA public key chain").

Note If the CA does not respond by a timeout period after this command is issued, the terminal control will be returned so that it remains available. If this happens, you must reenter the command. Cisco IOS software will not recognize CA certificate expiration dates set for beyond the year 2049. If the validity period of the CA certificate is set to expire after the year 2049, the following error message will be displayed when authentication with the CA server is attempted:

```
error retrieving certificate :incomplete chain
```

If you receive an error message similar to this one, check the expiration date of your CA certificate. If the expiration date of your CA certificate is set after the year 2049, you must reduce the expiration date by a year or more.

Examples

In the following example, the router requests the certificate of the CA. The CA sends its certificate and the router prompts the administrator to verify the certificate of the CA by checking the CA certificate's fingerprint. The CA administrator can also view the CA certificate's fingerprint, so you should compare what the CA administrator sees to what the router displays on the screen. If the fingerprint on the router's screen matches the fingerprint viewed by the CA administrator, you should accept the certificate as valid.

```
Router(config)# crypto pki authenticate myca

Certificate has the following attributes:
Fingerprint: 0123 4567 89AB CDEF 0123
Do you accept this certificate? [yes/no] y#
```

Related Commands

Command	Description
debug crypto pki transactions	Displays debug messages for the trace of interaction (message type) between the CA and the router.
enrollment	Specifies the enrollment parameters of your CA.
show crypto pki certificates	Displays information about your certificate, the certificate of the CA, and any RA certificates.

crypto pki benchmark

To start or stop benchmarking data for Public Key Infrastructure (PKI) performance monitoring and optimization, use the **crypto pki benchmark** command in privileged EXEC mode.

crypto pki benchmark {**start** *limit* [**wrap**] | **stop**}

Syntax Description

start *limit*	Enables PKI benchmarking. The *limit* argument states the number of records from 0 to 9990 that can be stored for the benchmarking session. A limit of 0 indicates an unlimited number of records can be stored.
wrap	(Optional) Specifies a continuous flow of records. Once the maximum number of records is gathered, they are released and a new set of records is generated. If the **wrap** keyword is not specified, then benchmarking stops once the limit for the maximum number of records has been reached.
stop	Terminates PKI benchmarking data collection.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Use the **crypto pki benchmark start** command to start the collection of PKI benchmarking performance monitoring and optimization data. Use the **crypto pki benchmark stop** command to stop the collection of the PKI benchmarking performance monitoring and optimization data.

Use the **show crypto pki benchmarks** command to view the collection data.

Use the **clear crypto pki benchmarks** command to clear the PKI benchmarking performance monitoring and optimization data and release all memory associated with this data.

The IOS PKI Performance Monitoring and Optimization feature enables you to collect the following types of PKI performance data:

- Time to validate entire certificate chain.
- Time to verify each certificate.
- Time to check revocation status for each certificate.
- Time to fetch certificate revocation list (CRL) database for each fetch location.
- Time to fetch Simple Certificate Enrollment Protocol (SCEP) method capabilities to retrieve the CRL.
- Time to process each CRL.
- Time to process the Online Certificate Status Protocol (OCSP) response. OCSP is a certificate revocation mechanism.
- Time to fetch Authentication, Authorization, and Accounting (AAA).

- CRL size.
- Validation result.
- Validation Bypass (pubkey cached).
- Method used to fetch a CRL.
- PKI session identifier.
- Crypto engine used (hardware, software, etoken).

Examples

The following example starts PKI benchmarking data and collects 20 records. Once 20 records are collected, they are released and a new set of 20 records is generated.

```
Router# crypto pki benchmark start 20 wrap
```

Related Commands

Command	Description
clear crypto pki benchmarks	Clears PKI benchmarking performance monitoring and optimization data and releases all memory associated with this data.
show crypto pki benchmarks	Displays benchmarking data for PKI performance monitoring and optimization that was collected.

crypto pki cert validate

To determine if a trustpoint has been successfully authenticated, a certificate has been requested and granted, and if the certificate is currently valid, use the **crypto pki cert validate** command in global configuration mode.

crypto pki cert validate *trustpoint*

Syntax Description

trustpoint	The trustpoint to be validated.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced. Also, effective with Cisco IOS Release 12.3(8)T, this command replaced the **crypto ca cert validate** command.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **crypto pki cert validate** command validates the router's own certificate for a given trustpoint. Use this command as a sanity check after enrollment to verify that the trustpoint is properly authenticated, a certificate has been requested and granted for the trustpoint, and that the certificate is currently valid. A certificate is valid if it is signed by the trustpoint certification authority (CA), not expired, and so on.

Examples

The following examples show the possible output from the **crypto pki cert validate** command:

```
Router(config)# crypto pki cert validate ka

Validation Failed: trustpoint not found for ka


Router(config)# crypto pki cert validate ka

Validation Failed: can't get local certificate chain


Router(config)# crypto pki cert validate ka

Certificate chain has 2 certificates.
Certificate chain for ka is valid


Router(config)# crypto pki cert validate ka
```

```
Certificate chain has 2 certificates.
Validation Error: no certs on chain


Router(config)# crypto pki cert validate ka

Certificate chain has 2 certificates.
Validation Error: unspecified error
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the certification authority that the router should use.
show crypto pki trustpoints	Displays the trustpoints that are configured in the router.

crypto pki certificate chain

To enter the certificate chain configuration mode, use the **crypto pki certificate chain** command in global configuration mode.

crypto pki certificate chain *name*

Syntax Description

name	Specifies the name of the certificate authority (CA). The name must match that which was declared for the CA using the **crypto pki trustpoint** command.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	The **crypto ca certificate chain** command was introduced.
12.3(7)T	This command replaced the **crypto ca certificate chain** command.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.4(2)T	The command output was modified to distinguish the current active certificate and the rollover certificate in the certificate chain.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command puts you into certificate chain configuration mode. When you are in certificate chain configuration mode, you can delete certificates using the **certificate** command.

You need to be in certificate chain configuration mode to delete certificates.

Examples

The following example deletes the router's certificate. In this example, the router had a general-purpose RSA key pair with one corresponding certificate. The show command is used to determine the serial number of the certificate to be deleted.

```
Router# show crypto pki certificates

Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: 0123456789ABCDEF0123456789ABCDEF
  Key Usage: General Purpose

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

```
Router# configure terminal
Router(config)# crypto pki certificate chain myca
Router(config-cert-chain)# no certificate 0123456789ABCDEF0123456789ABCDEF
% Are you sure you want to remove the certificate [yes/no]? yes
% Be sure to ask the CA administrator to revoke this certificate.
Router(config-cert-chain)# exit
```

The following example shows a certificate chain with an active CA certificate and a shadow, or rollover, certificate:

```
Router# configure terminal
Router(config)# crypto pki certificate chain myca

certificate 06

certificate ca 01

certificate rollover 0B
 ! This is the peer's shadow PKI certificate.

certificate rollover ca 0A
! This is the CA shadow PKI certificate
```

This example shows how the certificate chain is rewritten when rollover actually happens:

```
Router# configure terminal
Router(config)# crypto pki certificate chain myca

 certificate 0B
 certificate ca 0A
```

Related Commands

Command	Description
certificate	Adds certificates manually.

crypto pki certificate map

To define certificate-based access control lists (ACLs), use the **crypto pki certificate map** command in ca-certificate-map configuration mode. To remove the certificate-based ACLs, use the **no** form of this command.

crypto pki certificate map *label sequence-number*

no crypto pki certificate map *label sequence-number*

Syntax Description

label	A user-specified label that is referenced within the **crypto pki trustpoint** command.
sequence-number	A number that orders the ACLs with the same label. ACLs with the same label are processed from lowest to highest sequence number. When an ACL is matched, processing stops with a successful result.

Defaults

None

Command Modes

Ca-certificate-map configuration (ca-certificate-map)

Command History

Release	Modification
12.2(15)T	The **crypto ca certificate map** command was introduced.
12.3(7)T	This command replaced the **crypto ca certificate map** command.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(9)T	The **serial-number** field name was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

Issuing this command places the router in ca-certificate-map configuration mode where you can specify several certificate fields together with their matching criteria. The general form of these fields is as follows:

```
field-name match-criteria match-value
```

The *field-name* field in the above example is one of the certificate fields. Field names are similar to the names used in the ITU-T X.509 standard. The *field-name* is a special field that matches any subject name or related name field in the certificate, such as the **alt-subject-name, subject-name**, and **unstructured-subject-name** fields.

- **alt-subject-name**—Case-insensitive string.
- **expires-on**—Date field in the format dd mm yyyy hh:mm:ss or mmm dd yyyy hh:mm:ss.
- **issuer-name**—Case-insensitive string.
- **name**—Case-insensitive string.

- **serial-number**—Case-insensitive string.
- **subject-name**—Case-insensitive string.
- **unstructured-subject-name**—Case-insensitive string.
- **valid-start**—Date field in the format dd MM. yyy hh:mm:ss or mmm dd yyyy hh:mm:ss.

Note The time portion is optional in both the **expires-on** date and **valid-start** field and defaults to 00:00:00 if not specified. The time is interpreted according to the time zone offset configured for the router. The string **utc** can be appended to the date and time when they are configured as Universal Time, Coordinated (UTC) rather than local time.

The *match-criteria* field in the example is one of the following logical operators:

- **eq**—equal (valid for name and date fields)
- **ne**—not equal (valid for name and date fields)
- **co**—contains (valid only for name fields)
- **nc**—does not contain (valid only for name fields)
- **lt**—less than (valid only for date fields)
- **ge**—greater than or equal to (valid only for date fields)

The *match-value* field is a case-insensitive string or a date.

Examples

The following example shows how to configure a certificate-based ACL that will allow any certificate issued by Company to an entity within the company.com domain. The label is Company, and the sequence is 10.

```
crypto pki certificate map Company 10
 issuer-name co Company
 unstructured-subject-name co company.com
```

The following example accepts any certificate issued by Company for an entity with DIAL or organizationUnit component ou=WAN. This certificate-based ACL consists of two separate ACLs tied together with the common label Group. Because the check for DIAL has a lower sequence number, it is performed first. Note that the string “DIAL” can occur anywhere in the subjectName field of the certificate, but the string WAN must be in the organizationUnit component.

```
crypto pki certificate map Group 10
 issuer-name co Company
 subject-name co DIAL
crypto pki certificate map Group 20
 issuer-name co Company
 subject-name co ou=WAN
```

Case is ignored in string comparisons; therefore, DIAL in the previous example will match dial, DIAL, Dial, and so on. Also note that the component identifiers (o=, ou=, cn=, and so on) are not required unless it is desirable that the string to be matched occurs in a specific component of the name. (Refer to the ITU-T security standards for more information about certificate fields and components such as ou=.)

If a component identifier is specified in the match string, the exact string, including the component identifier, must appear in the certificate. This requirement can present a problem if more than one component identifier is included in the match string. For example, “ou=WAN,o=Company” will not match a certificate with the string “ou=WAN,ou=Engineering,o=Company” because the “ou=Engineering” string separates the two desired component identifiers.

To match both “ou=WAN” and “o=Company” in a certificate while ignoring other component identifiers, you could use this certificate map:

```
crypto pki certificate map Group 10
 subject-name co ou=WAN
 subject-name co o=Company
```

Any space character proceeding or following the equal sign (=) character in component identifiers is ignored. Therefore “o=Company” in the proceeding example will match “o = Company,” “o =Company,” and so on.

The following example shows a CA map file used to certificate serial number session control:

```
crypto pki trustpoint CA1
  enrollment url http://CA1
  ip-address FastEthernet0/0
  crl query ldap://CA1_ldap
  revocation-check crl
  match certificate crl-map1

  crypto pki certificate map crl-map1 1
  serial-number ne 489d
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the CA that your router should use.

crypto pki certificate query (ca-trustpoint)

To specify that certificates should not be stored locally but retrieved from a certification authority (CA) trustpoint, use the **crypto pki certificate query** command in ca-trustpoint configuration mode. To cause certificates to be stored locally per trustpoint, use the **no** form of this command.

crypto pki certificate query

no crypto pki certificate query

Syntax Description

This command has no arguments or keywords.

Defaults

CA trustpoints are stored locally in the router's NVRAM.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	The **crypto ca certificate query (ca-trustpoint)** command was introduced.
12.3(7)T	This command replaced the **crypto ca certificate query (ca-trustpoint)** command.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Normally, certain certificates are stored locally in the router's NVRAM, and each certificate uses a moderate amount of memory. To save NVRAM space, you can use this command to put the router into query mode, preventing certificates from being stored locally; instead, they are retrieved from a specified CA trustpoint when needed. This will save NVRAM space but could result in a slight performance impact.

The **crypto pki certificate query** command is a subcommand for each trustpoint; thus, this command can be disabled on a per-trustpoint basis.

Before you can configure this command, you must enable the **crypto pki trustpoint** command, which puts you in ca-trustpoint configuration mode.

Note This command deprecates the **crypto ca certificate query** command in global configuration mode. Although you can still enter the global configuration command, the configuration mode and command will be written back as ca-trustpoint.

Examples

The following example shows how to prevent certificates and certificate revocation lists (CRLs) from being stored locally on the router; instead, they are retrieved from the "ka" trustpoint when needed.

```
crypto pki trustpoint ka
 .
 .
 .
 crypto pki certificate query
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the CA that your router should use.

crypto pki certificate storage

To specify the local storage location for public key infrastructure (PKI) credentials, use the **crypto pki certificate storage** command in global configuration mode. To restore the default behavior, that is to store PKI credentials to NVRAM, use the **no** form of this command.

crypto pki certificate storage *location-name*

no crypto pki certificate storage

Syntax Description

location-name	Name of the local storage device. • Default is NVRAM.

Defaults

NVRAM is the default local storage location if this command is not issued.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

All Cisco platforms support NVRAM and flash local storage. Depending on your platform, you may have other supported local storage options including bootflash, slot, disk, USB flash, or USB token.

During run time, you can specify what active local storage device you would like to use to store PKI credentials. You must have the following system requirements before you can specify PKI credentials local storage location:

- A Cisco IOS Release 12.4(2)T PKI-enabled image or a later image
- A platform that supports storing PKI credentials as separate files
- A configuration that contains at least one certificate
- An accessible local file system

When using a local storage device to store PKI data, the following restrictions are applicable:

- Only local file systems may be used. An error message will be displayed if a remote file system is selected, and the command will not take effect.
- A subdirectory may be specified if supported by the local file system. NVRAM does not support subdirectories.
- Settings will take effect only when the running configuration is saved to the startup configuration.

If the keys are generated on the etoken, then the default storage loaction for the certificates is the etoken

for the device certificates. The CA certificates are stored in NVRAM. This allows for the credentials(keysa nd certificates) to be stored together on the removable media by default.

Examples

The following configuration example shows how to store certificates to the certs subdirectory. The certs subdirectory does not exist and is automatically created.

```
Router# dir nvram:

 114  -rw-        4687                    <no date>  startup-config
 115  ----        5545                    <no date>  private-config
 116  -rw-        4687                    <no date>  underlying-config
   1  ----          34                    <no date>  persistent-data
   3  -rw-         707                    <no date>  ioscaroot#7401CA.cer
   9  -rw-         863                    <no date>  msca-root#826E.cer
  10  -rw-         759                    <no date>  msca-root#1BA8CA.cer
  11  -rw-         863                    <no date>  msca-root#75B8.cer
  24  -rw-        1149                    <no date>  storagename#6500CA.cer
  26  -rw-         863                    <no date>  msca-root#83EE.cer

129016 bytes total (92108 bytes free)

Router# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# crypto pki certificate storage disk0:/certs
Requested directory does not exist -- created
Certificates will be stored in disk0:/certs/

Router(config)# end
Router# write
*May 27 02:09:00:%SYS-5-CONFIG_I:Configured from console by consolemem
Building configuration...
[OK]

Router# directory disk0:/certs

Directory of disk0:/certs/

  14  -rw-         707  May 27 2005 02:09:02 +00:00  ioscaroot#7401CA.cer
  15  -rw-         863  May 27 2005 02:09:02 +00:00  msca-root#826E.cer
  16  -rw-         759  May 27 2005 02:09:02 +00:00  msca-root#1BA8CA.cer
  17  -rw-         863  May 27 2005 02:09:02 +00:00  msca-root#75B8.cer
  18  -rw-        1149  May 27 2005 02:09:02 +00:00  storagename#6500CA.cer
  19  -rw-         863  May 27 2005 02:09:02 +00:00  msca-root#83EE.cer

47894528 bytes total (20934656 bytes free)


! The certificate files are now on disk0/certs:
```

Related Commands

Command	Description
show crypto pki certificates storage	Displays the current PKI certificate storage location.

crypto pki crl cache

To set the maximum amount of volatile memory used to cache certificate revocation lists (CRLs), use the **crypto pki crl cache** command in privileged EXEC mode. To restore the default value, use the **no** form of this command.

crypto pki crl cache *cache-size*

no crypto pki crl cache *cache-size*

Syntax Description

cache-size	The maximum CRL cache size in kilobytes. • The default value is 512 kilobytes. The value specified must be an integer. Specifying a cache size of zero disables CRL caching.

Command Default

The default CRL cache size is set to 512 kilobytes.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

The CRL cache is a global cache that holds all CRLs downloaded by the router regardless of the trustpoint configuration. The impact on router memory depends upon the CRL cache size configured by the administrator. Configuring the CRL cache size allows the amount of memory used for the CRL cache to be reduced (for instance, if low memory conditions exist) or to be increased for better performance (for instance, when a large number of CRLs are being processed).

If the **crypto pki crl cache** command is issued, regardless of the CRL cache size value set, the CRL cache size will be included in the configuration. Issuing the **no crypto pki crl cache** command will remove the CRL cache size from the configuration.

When a CRL is stored in the CRL cache, it is condensed at least one-fifth of its original size. Therefore, more CRLs can be stored in the CRL cache than would be expected based on the CRL size before being cached.

Note To configure CRL caching for a given trustpoint, you may issue either the **crl-cache none** or **crl cache delete-after** command. To disable caching of CRLs for a given trustpoint, use the **crl-cache none** command. To set a maximum age for CRLs in the cache for a given trustpoint, use the **crl cache delete-after** command.

Examples

The following example sets the maximum CRL cache size to 2048 kilobytes and then shows sample output of the **show crypto pki crls** command:

```
Router# crypto pki crl cache 2048
Router# show crypto pki crls

     CRL Issuer Name:
           cn=ioscs,l=Anytown,c=US
           LastUpdate: 02:53:41 GMT Mar 6 2007
           NextUpdate: 02:53:41 GMT Mar 13 2007
           Retrieved from CRL Distribution Point:
                ** CDP Not Published - Retrieved via SCEP
     CRL DER is 475 bytes
     CRL is stored in parsed CRL cache
     Parsed CRL cache current size is 1705 bytes
     Parsed CRL cache maximum size is 2048 bytes
```

Related Commands

Command	Description
crl cache delete-after	Deletes a CRL from the cache after the specified number of minutes.
crl cache none	Disables caching of all CRLs.
crypto pki crl request	Requests that a new CRL be obtained immediately from the CA.
show crypto pki crls	Displays the current CRL on the router.

crypto pki crl request

To request that a new certificate revocation list (CRL) be obtained immediately from the certification authority, use the **crypto pki crl request** command in global configuration mode.

crypto pki crl request *name*

Syntax Description

name	Specifies the name of the CA. This is the same name used when the CA was declared with the **crypto pki trustpoint** command.

Defaults

Normally, the router requests a new CRL when it is verifying a certificate and there is no CRL cached.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	The **crypto ca crl request** command was introduced.
12.3(7)T	This command replaced the **crypto ca crl request** command.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

A CRL lists all the certificates of the network device that have been revoked. Revoked certificates will not be honored by your router; therefore, any IPSec device with a revoked certificate cannot exchange IP Security traffic with your router.

The first time your router receives a certificate from a peer, it will download a CRL from the CA. Your router then checks the CRL to make sure the certificate of the peer has not been revoked. (If the certificate appears on the CRL, it will not accept the certificate and will not authenticate the peer.)

A CRL can be reused with subsequent certificates until the CRL expires. If your router receives the certificate of a peer after the applicable CRL has expired, it will download the new CRL.

If your router has a CRL which has not yet expired, but you suspect that the contents of the CRL are out of date, use the **crypto pki crl request** command to request that the latest CRL be immediately downloaded to replace the old CRL.

This command is not saved to the configuration.

Note This command should be used only after the trustpoint is enrolled.

Examples

The following example immediately downloads the latest CRL to your router:

```
crypto pki crl request
```

crypto pki enroll

To obtain the certificates for your router from the certificate authority (CA), use the **crypto pki enroll** command in global configuration mode. To delete a current enrollment request, use the **no** form of this command.

crypto pki enroll *name*

no crypto pki enroll *name*

Syntax Description

name	The name of the CA. Use the same name as when you declared the CA using the **crypto pki trustpoint** command.

Defaults

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3T	The **crypto ca enroll** command was introduced.
12.3(7)T	This command replaced the **crypto ca enroll** command.
12.3(14)T	The command was modified to include self-signed certificate information.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

This command requests certificates from the CA for all of your router's Rivest, Shamir, and Adelmen (RSA) key pairs. This task is also known as enrolling with the CA. (Technically, enrolling and obtaining certificates are two separate events, but they both occur when this command is issued.)

Your router needs a signed certificate from the CA for each RSA key pairs of your router; if you previously generated general-purpose keys, this command obtains the one certificate corresponding to the one general-purpose RSA key pair. If you previously generated special-usage keys, this command obtains two certificates corresponding to each of the special-usage RSA key pairs.

If you already have a certificate for your keys you are prompted to remove the existing certificate first. (You can remove existing certificates with the **no certificate** command.)

The **crypto pki enroll** command is not saved in the router configuration.

Note If your router reboots after you issue the **crypto pki enroll** command but before you receive the certificates, you must reissue the command.

Note If you are using a Secure Shell (SSH) service, you should set up specific RSA key pairs (different private keys) for the trustpoint and the SSH service. (If the Public Key Infrastructure [PKI] and the SSH infrastructure share the same default RSA key pair, a temporary disruption of SSH service could occur. The RSA key pair could become invalid or change because of the CA system, in which case you would not be able to log in using SSH. You could receive the following error message: "key changed, possible security problem.")

Responding to Prompts

When you issue the **crypto pki enroll** command, you are prompted a number of times.

You are prompted to create a challenge password. This password can be up to 80 characters in length. This password is necessary in the event that you ever need to revoke your router's certificates. When you ask the CA administrator to revoke your certificate, you must supply this challenge password as a protection against fraudulent or mistaken revocation requests.

Note This password is not stored anywhere, so you need to remember this password.

If you lose the password, the CA administrator may still be able to revoke the router's certificate but will require further manual authentication of the router administrator identity.

You are also prompted to indicate whether your router's serial number should be included in the obtained certificate. The serial number is not used by IP Security (IPsec) or Internet Key Exchange, but may be used by the CA to either authenticate certificates or to later associate a certificate with a particular router. (Note that the serial number stored is the serial number of the internal board, not the one on the enclosure.) Ask your CA administrator if serial numbers should be included. If you are in doubt, include the serial number.

Normally, you would not include the IP address because the IP address binds the certificate more tightly to a specific entity. Also, if the router is moved, you would need to issue a new certificate. A router has multiple IP addresses, any of which might be used with IPsec.

If you indicate that the IP address should be included, you will then be prompted to specify the interface of the IP address. This interface should correspond to the interface that you apply your crypto map set to. If you apply crypto map sets to more than one interface, specify the interface that you name in the **crypto map local-address** command.

Examples

In the following example, a router with a general-purpose RSA key pair requests a certificate from the CA. When the router displays the certificate fingerprint, the administrator verifies this number by calling the CA administrator, which checks the number. The fingerprint is correct, so the router administrator accepts the certificate.

There can be a delay between when the router administrator sends the request and when the certificate is actually received by the router. The amount of delay depends on the CA method of operation.

```
Router(config)# crypto pki enroll myca
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password: <mypassword>
```

```
Re-enter password: <mypassword>

% The subject name in the certificate will be: myrouter.example.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: 03433678
% Include an IP address in the subject name [yes/no]? yes
Interface: ethernet0/0
Request certificate from CA [yes/no]? yes
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificates' command will also show the fingerprint.
```

Some time later, the router receives the certificate from the CA and displays the following confirmation message:

```
Router(config)#   Fingerprint: 01234567 89ABCDEF FEDCBA98 75543210

%CRYPTO-6-CERTRET: Certificate received from Certificate Authority

Router(config)#
```

If necessary, the router administrator can verify the displayed fingerprint with the CA administrator.

If there is a problem with the certificate request and the certificate is not granted, the following message is displayed on the console instead:

```
%CRYPTO-6-CERTREJ: Certificate enrollment request was rejected by Certificate Authority
```

The subject name in the certificate is automatically assigned to be the same as the RSA key pair's name. In the example, the RSA key pair was named "myrouter.example.com." (The router assigned this name.)

Requesting certificates for a router with special-usage keys would be the same as in the previous example, except that two certificates would have been returned by the CA. When the router received the two certificates, the router would have displayed the same confirmation message:

```
%CRYPTO-6-CERTRET: Certificate received from Certificate Authority
```

Related Commands

Command	Description
crypto map local address	Specifies and names an identifying interface to be used by the crypto map for IPsec traffic.
debug crypto pki messages	Displays debug messages for the details of the interaction (message dump) between the CA and the router.
debug crypto pki transactions	Displays debug messages for the trace of interaction (message type) between the CA and the router.
show crypto pki certificates	Displays information about your certificate, the certificate of the CA, and any RA certificates.

crypto pki export pem

To export certificates and Rivest, Shamir, and Adelman (RSA) keys that are associated with a trustpoint in a privacy-enhanced mail (PEM)-formatted file, use the **crypto pki export pem** command in global configuration mode.

crypto pki export *trustpoint* **pem** {**terminal** | **url** *url*} {**3des** | **des**} *passphrase* [**rollover**]

Syntax Description

trustpoint	Name of the trustpoint that the associated certificate and RSA key pair will export. The *trustpoint* argument must match the name that was specified via the **crypto pki trustpoint** command.
terminal	Certificate and RSA key pair that will be displayed in PEM format on the console terminal.
url *url*	URL of the file system where your router should export the certificate and RSA key pairs.
3des	Export the trustpoint using the Triple Data Encryption Standard (3DES) encryption algorithm.
des	Export the trustpoint using the DES encryption algorithm.
passphrase	Passphrase that is used to encrypt the PEM file for import. **Note** The passphrase can be any phrase that is at least eight characters in length; it can include spaces and punctuation, excluding the question mark (?), which has special meaning to the Cisco IOS parser.
rollover	(Optional) Export certificate authority (CA) shadow, or rollover, certificate.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	The **crypto ca export pem** command was introduced.
12.3(7)T	This command replaced the **crypto ca export pem** command.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.4(2)T	The **rollover** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **crypto pki export pem** command allows you to export certificate and RSA key pairs in PEM-formatted files. The PEM files can then be imported back into the Cisco IOS router (via the **crypto pki import pem** command) or other public key infrastructure (PKI) applications.

Examples

The following example shows how to generate and export the RSA key pair "aaa" and certificates of the router in PEM files that are associated with the trustpoint "mycs":

```
Router(config)# crypto key generate rsa general-keys label aaa exportable
The name for the keys will be:aaa
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes.
!
How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]
!
Router(config)# crypto pki trustpoint mycs
Router(ca-trustpoint)# enrollment url http://mycs
Router(ca-trustpoint)# rsakeypair aaa
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate mycs
Certificate has the following attributes:
Fingerprint:C21514AC 12815946 09F635ED FBB6CF31
% Do you accept this certificate? [yes/no]:y
Trustpoint CA certificate accepted.
!
Router(config)# crypto pki enroll mycs
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this password to the CA
Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.

Password:
Re-enter password:

% The fully-qualified domain name in the certificate will be:Router
% The subject name in the certificate will be:bizarro.cisco.com
% Include the router serial number in the subject name? [yes/no]:n
% Include an IP address in the subject name? [no]:n
Request certificate from CA? [yes/no]:y
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

Router(config)# Fingerprint: 8DA777BC 08477073 A5BE2403 812DD157

00:29:11:%CRYPTO-6-CERTRET:Certificate received from Certificate Authority

Router(config)# crypto pki export aaa pem terminal 3des cisco123

% CA certificate:
-----BEGIN CERTIFICATE-----
MIICAzCCAa2gAwIBAgIBATANBgkqhkiG9w0BAQUFADBOMQswCQYDVQQGEwJVUzES
<snip>
waDeNOSI3WlDa0AWq5DkVBkxwgn0TqIJXJOCttjHnWHK1LMcMVGn
-----END CERTIFICATE-----

% Key name:aaa
    Usage:General Purpose Key
-----BEGIN RSA PRIVATE KEY-----
Proc-Type:4,ENCRYPTED
DEK-Info:DES-EDE3-CBC,ED6B210B626BC81A

Urguv0jnjwOgowWVUQ2XR5nbzzYHI2vGLunpH/IxIsJuNjRVjbAAUpGk7VnPCT87
<snip>
kLCOtxzEv7JHc72gMku9uUlrLSnFH5slzAtoC0czfU4=
```

```
-----END RSA PRIVATE KEY-----

% Certificate:
-----BEGIN CERTIFICATE-----
MIICTjCCAfigAwIBAgICIQUwDQYJKoZIhvcNAQEFBQAwTjELMAkGA1UEBhMCVVMx
<snip>
6xlBaIsuMxnHmr89KkKkYlU6
-----END CERTIFICATE-----
```

Related Commands

Command	Description
crypto pki import pem	Imports certificates and RSA keys to a trustpoint from PEM-formatted files.
crypto pki trustpoint	Declares the CA that your router should use.
enrollment	Specifies the enrollment parameters of a CA.

crypto pki export pkcs12

To export Rivest, Shamir, and Adelman (RSA) keys within a PKCS12 file at a specified location, use the **crypto pki export pkcs12** command in global configuration mode.

crypto pki export *trustpointname* **pkcs12** *destination url passphrase*

Syntax Description

trustpointname	Name of the trustpoint who issues the certificate that a user is going to export. When you export the PKCS12 file, the trustpoint name is the RSA key name.
destination url	Location of the PKCS12 file to which a user wants to import the RSA key pair.
passphrase	Passphrase that is used to encrypt the PKCS12 file for export.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	The **crypto ca export pkcs12** command was introduced.
12.3(7)T	This command replaced the **crypto ca export pkcs12** command.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **crypto pki export pkcs12** command creates a PKCS 12 file that contains an RSA key pair. The PKCS12 file, along with a certificate authority (CA), is exported to the location that you specify with the destination URL. If you decide not to import the file to another router, you must delete the file.

Security Measures

Keep the PKCS12 file stored in a secure place with restricted access.

An RSA keypair is more secure than a passphrase because the private key in the key pair is not known by multiple parties. When you export an RSA key pair to a PKCS#12 file, the RSA key pair now is only as secure as the passphrase.

To create a good passphrase, be sure to include numbers, as well as both lowercase and uppercase letters. Avoid publicizing the passphrase by mentioning it in e-mail or cell phone communications because the information could be accessed by an unauthorized user.

Examples

The following example exports an RSA key pair with a trustpoint name “mytp” to a Flash file:

```
Router(config)# crypto pki export mytp pkcs12 flash:myexport mycompany
```

Related Commands

Command	Description
crypto pki import pkcs12	Imports RSA keys.

crypto pki import

To import a certificate manually via TFTP or as a cut-and-paste at the terminal, use the **crypto pki import** command in global configuration mode.

crypto pki import *name* **certificate**

Syntax Description

name **certificate**	Name of the certification authority (CA). This name is the same name used when the CA was declared with the **crypto pki trustpoint** command.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	The **crypto ca import** command was introduced.
12.3(7)T	This command replaced the **crypto ca import** command.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

You must enter the **crypto pki import** command twice if usage keys (signature and encryption keys) are used. The first time the command is entered, one of the certificates is pasted into the router; the second time the command is entered, the other certificate is pasted into the router. (It does not matter which certificate is pasted first.)

Examples

The following example shows how to import a certificate via cut-and-paste. In this example, the CA trustpoint is "MS."

```
crypto pki trustpoint MS
 enroll terminal
 crypto pki authenticate MS
!
crypto pki enroll MS
crypto pki import MS certificate
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the CA that your router should use.
enrollment	Specifies the enrollment parameters of your CA.
enrollment terminal	Specifies manual cut-and-paste certificate enrollment.

crypto pki import pem

To import certificates and Rivest, Shamir, and Adelman (RSA) keys to a trustpoint from privacy-enhanced mail (PEM)-formatted files, use the **crypto pki import pem** command in global configuration mode.

crypto pki import *trustpoint* **pem** [**usage-keys**] {**terminal** | **url** *url*} [**exportable**] *passphrase*

Syntax Description

trustpoint	Name of the trustpoint that is associated with the imported certificates and RSA key pairs. The *trustpoint* argument must match the name that was specified via the **crypto pki trustpoint** command.
usage-keys	(Optional) Specifies that two RSA special usage key pairs will be imported (that is, one encryption pair and one signature pair), instead of one general-purpose key pair.
terminal	Certificates and RSA key pairs will be manually imported from the console terminal.
url *url*	URL of the file system where your router should import the certificates and RSA key pairs.
exportable	(Optional) Specifies that the imported RSA key pair can be exported again to another Cisco device such as a router.
passphrase	Passphrase that is used to encrypt the PEM file for import. **Note** The passphrase can be any phrase that is at least eight characters in length; it can include spaces and punctuation, excluding the question mark (?), which has special meaning to the Cisco IOS parser.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	The **crypto ca import pem** command was introduced.
12.3(7)T	This command replaced the **crypto ca import pem** command.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **crypto pki import pem** command allows you import certificates and RSA key pairs in PEM-formatted files. The files can be previously exported from another router or generated from other public key infrastructure (PKI) applications.

Examples

The following example shows how to import PEM files to trustpoint “ggg” via TFTP:

```
Router(config)# crypto pki import ggg pem url tftp://10.1.1.2/johndoe/msca cisco1234

% Importing CA certificate...
Address or name of remote host [10.1.1.2]?
Destination filename [johndoe/msca.ca]?
Reading file from tftp://10.1.1.2/johndoe/msca.ca
Loading johndoe/msca.ca from 10.1.1.2 (via Ethernet0):!
[OK - 1082 bytes]

% Importing private key PEM file...
Address or name of remote host [10.1.1.2]?
Destination filename [johndoe/msca.prv]?
Reading file from tftp://10.1.1.2/johndoe/msca.prv
Loading johndoe/msca.prv from 10.1.1.2 (via Ethernet0):!
[OK - 573 bytes]

% Importing  certificate PEM file...
Address or name of remote host [10.1.1.2]?
Destination filename [johndoe/msca.crt]?
Reading file from tftp://10.1.1.2/johndoe/msca.crt
Loading johndoe/msca.crt from 10.1.1.2 (via Ethernet0):!
[OK - 1289 bytes]
% PEM files import succeeded.
Router(config)#
```

Related Commands

Command	Description
crypto pki export pem	Exports certificates and RSA keys that are associated with a trustpoint in a PEM-formatted file.
crypto pki trustpoint	Declares the CA that your router should use.
enrollment	Specifies the enrollment parameters of a CA.

crypto pki import pkcs12

To import Rivest, Shamir, and Adelman (RSA) keys, use the **crypto pki import pkcs12** command in global configuration mode.

crypto pki import *trustpointname* **pkcs12** *source url passphrase*

Syntax Description

trustpointname	Name of the trustpoint who issues the certificate that a user is going to export or import. When importing, the trustpoint name will become the RSA key name.
source url	The location of the PKCS12 file to which a user wants to export the RSA key pair.
passphrase	Passphrase that must be entered to undo encryption when the RSA keys are imported.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	The **crypto ca import pkcs12** command was introduced.
12.3(7)T	This command replaced the **crypto ca import pkcs12** command.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When you enter the **crypto pki import pkcs12** command, a ke pair and a trustpoint are generated. If you then decide you want to remove the key pair and trustpoint that were generated, enter the **crypto key zeroize rsa** command to zeroize the key pair and enter the **no crypto pki trustpoint** command to remove the trustpoint.

Note After you import RSA keys to a target router, you cannot export those keys from the target router to another router.

Examples

In the following example, an RSA key pair that has been associated with the trustpoint “forward” is to be imported:

```
Router(config)# crypto pki import forward pkcs12 flash:myexport mycompany
```

Related Commands

Command	Description
crypto pki export pkcs12	Exports RSA keys.
crypto pki trustpoint	Declares the CA that your router should use.
crypto key zeroize rsa	Deletes all RSA keys from your router.

crypto pki profile enrollment

To define an enrollment profile, use the **crypto pki profile enrollment** command in global configuration mode. To delete all information associated with this enrollment profile, use the **no** form of this command.

crypto pki profile enrollment *label*

no crypto pki profile enrollment *label*

Syntax Description

label	Name for the enrollment profile; the enrollment profile name must match the name specified in the **enrollment profile** command.

Defaults

An enrollment profile does not exist.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(7)T	This command replaced the **crypto ca profile enrollment** command.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Before entering this command, you must specify a named enrollment profile using the **enrollment profile** in ca-trustpoint configuration mode.

After entering the **crypto pki profile enrollment** command, you can use any of the following commands to define the profile parameters:

- **authentication command**—Specifies the HTTP command that is sent to the certification authority (CA) for authentication.
- **authentication terminal**—Specifies manual cut-and-paste certificate authentication requests.
- **authentication url**—Specifies the URL of the CA server to which to send authentication requests.
- **enrollment command**—Specifies the HTTP command that is sent to the CA for enrollment.
- **enrollment terminal**—Specifies manual cut-and-paste certificate enrollment.
- **enrollment url**—Specifies the URL of the CA server to which to send enrollment requests.
- **parameter**—Specifies parameters for an enrollment profile. This command can be used only if the **authentication command** or the **enrollment command** is used.

Note The **authentication url**, **enrollment url**, **authentication terminal**, and **enrollment terminal** commands allow you to specify different methods for certificate authentication and enrollment, such as TFTP authentication and manual enrollment.

Examples

The following example shows how to define the enrollment profile named "E" and associated profile parameters:

```
crypto pki trustpoint Entrust
  enrollment profile E
  serial

crypto pki profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the PKI trustpoint that your router should use.
enrollment profile	Specifies that an enrollment profile can be used for certificate authentication and enrollment.

crypto pki server

To enable a Cisco IOS certificate server and enter certificate server configuration mode or to immediately generate shadow certification authority (CA) credentials, use the **crypto pki server** command in global configuration mode. To disable a certificate server (which is the default functionality), use the **no** form of this command.

crypto pki server *cs-label* [**rollover** [**cancel**] [**request pkcs10 terminal**]] [**redundancy**] [**show**] [**serial-number** *serial-number*]

no crypto pki server *cs-label*

Syntax Description

cs-label	Name of the certificate server. **Note** The certificate server name should not exceed 13 characters.
rollover	(Optional) Immediately generates a shadow CA certificate. **Note** If the **auto-enroll** command has been issued with the **regenerate** keyword, shadow keys will also be generated. **Note** If the shadow certificate and keys are already present this command will fail.
cancel	(Optional) Deletes the exiting shadow CA certificate when used with the **rollover** keyword. Shadow keys will also be deleted if they exist.
request pkcs10 terminal	(Optional) Exports CA shadow certificate. Also exports shadow keys if they exist.
redundancy	(Optional) Synchronizes the server configuration with that of the standby CA.
show	(Optional) Displays the current configuration of the server being configured.
serial-number *serial-number*	(Optional) Specifies the next serial number to be issued, and updates the serial-number file.

Defaults

A certificate server is not enabled; the automatic CA certificate rollover process is not initiated.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(2)T	The **rollover**, **cancel**, and **request pkcs10 terminal** keywords were introduced to support automated CA certificate rollover functionality.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)M	This command was modified. The **redundancy**, **show**, and **serial-number** keywords were added.

Usage Guidelines

A certificate server allows you to more easily deploy public key infrastructure (PKI) by defining default behavior, which limits user interface complexity. To define the functionality of the certificate server, you can use any of the following certificate server configuration mode commands:

- **database (certificate server)**—Requires a username or password to be issued when accessing a database storage location.
- **database level**—Controls what type of data is stored in the certificate enrollment database.
- **database url**—Specifies the location where all database entries for the certificate server will be written out.
- **grant automatic**—Specifies automatic certificate enrollment.

Note This command can be used for testing and building simple networks; however, it is recommended that you do not issue this command if your network is generally accessible.

- **issuer-name**—Specifies the distinguished name (DN) as the CA issuer name for the certificate server.
- **lifetime (certificate server)**—Specifies the lifetime of the CA or a certificate.
- **lifetime crl**—Defines the lifetime of the certificate revocation list (CRL) that is used by the certificate server.
- **shutdown**—Allows a certificate server to be disabled without removing the configuration.

Note All of these commands are optional; thus, any basic certificate server functionality that is not specified via the command-line interface (CLI) will use the default value.

Automated CA Certificate Rollover

CAs and their clients, have certificates with expiration dates that have to be reissued when the current certificate is about to expire. CAs also have key pairs used to sign client certificates. When the CA certificate is expiring it must generate a new certificate and possibly a new key pair. This process, called rollover, allows for continuous operation of the network while clients and the certificate server are switching from an expiring CA certificate to a new CA certificate.

Examples

The following example shows how to enable the certificate server “mycertserver”:

```
Router(config)# ip http server
Router(config)# crypto pki server mycertserver
Router(cs-server)# database url tftp://mytftp/johndoe/mycertserver
```

The following example shows how to disable the certificate server “mycertserver”:

```
Router(config)# no crypto pki server mycertserver
% This will stop the Certificate Server process and delete the server
  configuration
Are you sure you want to do this? [yes/no]: yes
% Do you also want to remove the associated trustpoint and
  signing certificate and key? [yes/no]: no
% Certificate Server Process stopped
```

The following example shows a shadow client certificate request from a terminal:

```
Router# crypto pki server mycs rollover request pkcs10 terminal

% Enter Base64 encoded or PEM formatted PKCS10 enrollment request.

% End with a blank line or "quit" on a line by itself.

-----BEGIN CERTIFICATE REQUEST-----

MIIBUTCBuwIBADASMRAwDgYDVQQDEwdOZXdSb290MIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDMHeev1ERSs320zbLQQk+3lhV/R2HpYQ/iM6uT1jkJf5iy0UPR
wF/X16yUNmG+ObiGiW9fsASF0nxZw+fO7d2X2yh1PakfvF2wbP27C/sgJNOw9uPf
sBxEc40Xe0d5FMh0YKOSAShfZYKOflnyQR2Drmm2x/33QGol5QyRvjkeWQIDAQAB
oAAwDQYJKoZIhvcNAQEEBQADgYEALM90r4d79X6vxhD0qjuYJXfBCOvv4FNyFsjr
aBS/y6CnNVYySF8UBUohXYIGTWf4I4+sj6i8gYfoFUW1/L82djS18TLrUr6wpCOs
RqfAfps7HW1e4cizOfjAUU+C7lNcobCAhwF1o6q2nIEjpQ/2yfK9O7sb3SCJZBfe
eW3tyCo=

-----END CERTIFICATE REQUEST-----
```

The following example shows the **redundancy**, **show**, and **serial-number** keywords in the **crypto pki server** command.

```
Router(config)#crypto pki server MYCA
Router(cs-server)#grant auto
Router(cs-server)#redundancy
Router(cs-server)#serial-number 0x4c
Router(cs-server)#show
 redundancy
 serial-number 0x4C
 grant auto
end
```

Related Commands

Command	Description
crypto pki server info requests	Displays all outstanding certificate enrollment requests.
ip http server	Enables an HTTP server on your network.

crypto pki server grant

To grant all or certain simple certificate enrollment protocol (SCEP) requests, use the **crypto pki server grant** command in privileged EXEC mode.

crypto pki server *cs-label* **grant** {**all** | *req-id*}

Syntax Description

cs-label	Name of the certificate server. The name must match the name specified via the **crypto pki server** command.
all	All certificate enrollment requests are granted.
req-id	ID associated with a specific enrollment request in the enrollment request database. Use the **crypto pki server info requests** command to display the ID.

Defaults

If this command is not issued, the certificate server keeps the requests in a pending state.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

After you enable the **crypto pki server grant** command, your certificate server will immediately grant all specified certificate requests. Certificate requests that are not granted will expire after the time that was specified using the **lifetime enrollment-request** command.

Examples

The following example shows to grant all manual enrollment requests for the certificate server "mycs":

```
Router# crypto pki server mycs grant all
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.
crypto pki server reject	Rejects all or certain SCEP requests.

crypto pki server info crl

Note Effective with Cisco IOS Release 12.4(20)T, the **crypto pki server info crl** command is replaced by the **show crypto pki server crl** command. See the **show crypto pki server crl** command for more information.

To display information regarding the status of the current certificate revocation list (CRL), use the **crypto pki server info crl** command in privileged EXEC mode.

crypto pki server *cs-label* **info crl**

Syntax Description

cs-label	Name of the certificate server. The name must match the name specified via the **crypto pki server** command.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(20)T	This command was replaced by the **show crypto pki server crl** command.

Usage Guidelines

CRLs are issued once every specified time period via the **lifetime crl** command. It is the responsibility of the network administrator to ensure that the CRL is available from the location that is specified via the **cdp-url** command. To access information, such as the lifetime and location of the CRL, use the **crypto pki server info crl** command.

Examples

The following example shows how to access CRL information for the certificate server “mycs”:

```
Router# crypto pki server mycs info crl
```

Related Commands

Command	Description
cdp-url	Specifies a CDP to be used in certificates that are issued by the certificate server.
crypto pki server	Enables a Cisco IOS certificate server and enter certificate server configuration mode.
lifetime crl	Defines the lifetime of the CRL that is used by the certificate server.

crypto pki server info requests

Note Effective with Cisco IOS Release 12.4(20)T, the **crypto pki server info requests** command is replaced by the **show crypto pki server requests** command. See the **show crypto pki server requests** command for more information.

To display all outstanding certificate enrollment requests, use the **crypto pki server info requests** command in privileged EXEC mode.

crypto pki server *cs-label* **info requests**

Syntax Description

cs-label	Name of the certificate server. The name must match the name specified via the **crypto pki server** command.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(2)T	The command output was modified to include shadow CA certificate information.
12.4(20)T	This command was replaced by the **show crypto pki server requests** command.

Usage Guidelines

A certificate enrollment request functions as follows:

- The certificate server receives the enrollment request from an end user, and the following actions occur:
  - A request entry is created in the enrollment request database with the initial state. (See the **show pki server** command for a complete list of certificate enrollment request states.)
  - The certificate server refers to the command-line interface (CLI) configuration (or the default behavior any time a parameter is not specified) to determine the authorization of the request. Thereafter, the state of the enrollment request is updated in the enrollment request database.
- At each Simple Certificate Enrollment Protocol (SCEP) query for a response, the certificate server examines the current request and performs one of the following actions:
  - Responds to the end user with a “pending” or “denied” state.
  - Forwards to the request to the certification authority (CA) core, where it will generate and sign the appropriate certificate, store the certificate in the enrollment request database, and return the request to the built-in certificate server SCEP server, who will reply to the end user with the certificate on the next SCEP request.

If the connection of the client has closed, the certificate server will wait for client user to request another certificate.

All enrollment requests transitions through the certificate enrollment states that are defined in Table 27.

Table 27 Certificate Enrollment Request State Descriptions

Certificate Enrollment State	Description
initial	The request has been created by the SCEP server.
authorized	The certificate server has authorized the request.
malformed	The certificate server has determined that the request is invalid for cryptographic reasons.
denied	The certificate server has denied the request for policy reasons.
pending	The enrollment request must be manually accepted by the network administrator.
granted	The CA core has generated the appropriate certificate for the certificate request.

Examples

The following example shows output for the certificate server "certsrv1," which has a pending certificate enrollment request:

```
Router# crypto pki server certsrv1 info requests

   Enrollment Request Database:
   ReqID  State      Fingerprint                      SubjectName
   --------------------------------------------------------------
   1      pending    0A71820219260E526D250ECC59857C2D serialNumber=2326115A+hostname=831.
```

The following example shows the output for shadow PKI certificate info requests:

```
Router# crypto pki server mycs info requests

Enrollment Request Database:

RA certificate requests:

  ReqID  State      Fingerprint                      SubjectName

--------------------------------------------------------------
RA rollover certificate requests:

  ReqID  State      Fingerprint                      SubjectName

  --------------------------------------------------------------

Router certificates requests:

  ReqID  State      Fingerprint                      SubjectName

--------------------------------------------------------------

1      pending    A426AF07FE3A4BB69062E0E47198E5BF hostname=client

  Router rollover certificates requests:
```

```
ReqID  State      Fingerprint                      SubjectName

--------------------------------------------------------------

2      pending    B69062E0E47198E5BFA426AF07FE3A4B hostname=client
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters PKI configuration mode.

crypto pki server password generate

To generate a password for simple certificate enrollment protocol (SCEP) requests that can be used only one time, use the **crypto pki server password generate** command in privileged EXEC mode.

crypto pki server *cs-label* **password generate** [*minutes*]

Syntax Description

cs-label	Name of the certificate server. The name must match the name specified via the **crypto pki server** command.
minutes	(Optional) Length of time, in minutes, that the password is valid. Valid times range from 1 to 1440 minutes. The default value is 60 minutes.

Defaults

If this command is not enabled, no password is created.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

SCEP, which is the only supported enrollment protocol, supports two client authentication mechanisms—manual and preshared key. Manual enrollment requires the administrator at the certification authority (CA) server to specifically authorize the enrollment requests; enrollment using preshared keys allows the administrator to preauthorize enrollment requests by generating a one-time password.

Note Only one password is valid at a time; if a second password is generated, the previous password is no longer valid.

Examples

The following example shows how to generate a one-time password that is valid for 75 minutes for the certificate server “mycs”:

```
Router# crypto pki server mycs password generate 75
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.

crypto pki server reject

To reject all or certain Simple Certificate Enrollment Protocol (SCEP) requests, use the **crypto pki server reject** command in privileged EXEC mode.

crypto pki server *cs-label* **reject** {**all** | *req-id*}

Syntax Description

cs-label	Name of the certificate server. The name must match the name specified via the **crypto pki server** command.
all	All certificate enrollment requests are rejected.
req-id	ID associated with a specific enrollment request in enrollment request database. Use the **crypto pki server info requests** command to display the ID.

Defaults

If this command is not issued, the certificate server keeps the requests in a pending state.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

After you enable the **crypto pki server reject** command, your certificate server will immediately reject all certificate requests.

SCEP, which is the only supported enrollment protocol, supports two client authentication mechanisms—manual and preshared key. Manual enrollment requires the administrator at the certification authority (CA) server to specifically authorize the enrollment requests. The administrator can become overloaded if there are numerous enrollment requests. Thus, the **crypto pki server reject** command can be reduce user interaction by automatically rejecting all or specific enrollment requests.

Examples

The following example shows how reject all manual enrollment requests for the certificate server "mycs":

```
Router# crypto pki server mycs reject all
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.
crypto pki server grant	Grants all or certain SCEP requests.
crypto pki server info requests	Displays all outstanding certificate enrollment requests.

crypto pki server remove

To remove enrollment requests that are in the certificate server Enrollment Request Database, use the **crypto pki server remove** command in privileged EXEC mode . This command does not have a **no** form.

crypto pki server *cs-label* **remove** {**all** | *req-id*}

Syntax Description

cs-label	Name of the certificate server.
all	Removes all enrollment requests.
req-id	Removes the specified enrollment request.

Defaults

Enrollment requests will remain in the certificate server database.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

After the certificate server receives an enrollment request, it can leave the request in pending, reject it, or grant it. Before this command was added, the request would be left in the Enrollment Request Database for 1 hour until the client polled the certficiate server for the result of the request. This command allows you to remove individual or all requests from the database, especially useful if the client leaves and never polls the certificate server.

In addition, the use of this command also allows the server to be returned to a clean slate with respect to the keys and transaction IDs. Thus, it is a useful command to use during troubleshooting with a Simple Certificate Enrollment Protocol (SCEP) client that may be behaving badly.

Examples

The following example shows that all enrollment requests are to be removed from the certificate server:

```
Router# enable
 Router# crypto pki server server1 remove all
```

Related Commands

Command	Description
crypto pki server info request	Displays all outstanding enrollment requests.

crypto pki server request pkcs10

To manually add a certificate request to the request database, use the **crypto pki server request pkcs10** command in privileged EXEC mode.

crypto pki server *cs-label* **request pkcs10** {*url* | **scep** | **terminal**} [**base64** | **pem** | **hex** [*transaction-id* [*nonce* [*request-id*]]]]

Syntax Description

cs-label	Name of the certificate server. The name must match the name specified through the **crypto pki server** command.
url	URL of the file systems from which the certificate server should retrieve the PKCS10 enrollment request and to which it should post the granted certificate. **Note** The request filename should have a ".req" extension and the granted certificate file name will have a ".crt" extension (see the URL example in the section "Examples" below).
scep	Specifies the certificate is returned using Secure Certificate Enrollment Protocol (SCEP) request.
terminal	Certificate requests is manually pasted from the console terminal, and the granted certificate is displayed on the console.
base64	(Optional) Specifies the certificate is returned *without* privacy-enhanced mail (PEM) headers, regardless of whether PEM headers were used in the request.
pem	(Optional) Specifies the certificate is returned *with* PEM headers automatically added to the certificate after the certificate is granted, regardless of whether PEM headers were used in the request.
hex	(Optional) Specifies the certificate is returned in hexadecimal. Pending requests will also be synchronized with the standby certificate server in hexadecimal.
transaction-id	(Optional) Transaction ID in hexadecimal format.
nonce	(Optional) Nonce word in hexadecimal format. (Nonce words frequently arise through the combination of an existing word with a familiar prefix or suffix, in order to meet a particular need)
request-id	(Optional) Request ID. Valid values are from 1 to 999.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.3(11)T	This command was modified. The **pem** keyword was added.

Release	Modification
12.4(6)T	This command was modified. The **base64** keyword was added.
15.0(1)M	This command was modified. The **scep** and **hex** keywords and *transaction-id*, *nonce*, and *request-id* arguments were added. Command accepts the PKCS10 certificate and the signing certificate in hexadecimal as well as in base64 encoding.
15.1(1)T	This command was modified. The prompt for entering a certificate in hex mode has changed from config-pubkey to config-pki-hexmode.

Usage Guidelines

Use the **crypto pki server request pkcs10** command to manually add a base64-encoded, PEM-formatted, or hexadecimal-encoded PKCS10 certificate enrollment request. This command is especially useful when the client does not have a network connection with the certificate server so that it can do Simple Certificate Enrollment Protocol (SCEP) enrollment. After the certificate is granted, the certificate will be displayed on the console terminal using base64 encoding if the **terminal** keyword is specified, or it will be sent to the file system that is specified using the *url* argument.

The *url* argument allows you to specify or change the location in which the certificate server retrieves the new certificate request and posts the granted certificate.

Examples

The following example shows how to manually add a base64-encoded certificate request with PEM boundaries to the request database:

```
Router# crypto pki server mycs request pkcs10 terminal pem

% Enter Base64 encoded or PEM formatted PKCS10 enrollment request.
% End with a blank line or "quit" on a line by itself.
-----BEGIN CERTIFICATE REQUEST-----
MIIBdTCB3wIBADA2MQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lzdGVt
czEPMA0GA1UEAxMGdGVzdCAxMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDF
EFukc2lCFSHtDJn6HFR2n8rpdhlAYwcs0m68N3iRYHonv847h0/H6utTHVd2qEEo
rNw97jMRZk6BLhVDc05TKGHvUlBlHQWwc/BqpVI8WiHzZdskUH/DUM8kd67Vkjlb
e+FF7WrWT4FIO4vR4rF1V2p3FZ+A29UNc9Pi1s98nQIDAQABoAAwDQYJKoZIhvcN
AQEEBQADgYEAUQCGNzzNJwBOCwmEmG8XEGFSZWDmFlctm8VWvaZYMPOt+vl6iwFk
RmtD1Kg91Vw/qT5FJN8LmGUopOWIrwH4rUWON+TqtRmv2dgsdL5T4dx0sgG5E0s4
T302paxEHiHVRJpe8OD7FJgOvdsKRziCpyD4/Jfb1WnSVQZmvIYAxVQ=
-----END CERTIFICATE REQUEST-----

% Enrollment request pending, reqId=2

Router# crypto pki server mycs grant 2
% Granted certificate:
-----BEGIN CERTIFICATE-----
MIIB/TCCAWagAwIBAgIBAzANBgkqhkiG9w0BAQQFADAPMQ0wCwYDVQQDEwRteWNz
MB4XDTA0MDgyODAxMTcyOVoXDTA1MDgyODAxMTcyOVowNjELMAkGA1UEBhMCVVMx
FjAUBgNVBAoTDUNpc2NvIFN5c3RlbXMxDzANBgNVBAMTBnRlc3QgMTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEAxRBbpHNpQhUh7QyZ+hxUdp/K6XYZQGMHLNJu
vDd4kWB6J7/OO4dPx+rrUx1XdqhBKKzcPe4zEWZOgS4VQ3NOUyhh71JQZR0FsHPw
aqVSPFoh82XbJFB/w1DPJHeu1ZI5W3vhRe1q1k+BSDuL0eKxdVdqdxWfgNvVDXPT
4tbPfJ0CAwEAAaNCMEAwHwYDVR0jBBgwFoAUggWpVwokbUtGIwGZGavh6C8Bq6Uw
HQYDVR0OBBYEFFD3jZ/d960qzCGKwKNtFvq85Xt6MA0GCSqGSIb3DQEBBAUAA4GB
AAE4MqerwbM/nO8BCyZAiDzTqwLGnNvzS4H+u3JCsm0LaxY+E3d8NbSY+HruXWaR
7QyjprDGFd9bftRoqGYuiQkupU13sIHEyf3C2KnXJB6imySvAiuaQrGdSuUSIhBO
Xfh/xdWo3XL1e3vtWiYUa4X6jPUMpn74HoNfB4/gHO7g
-----END CERTIFICATE-----
```

The following example shows how to retrieve a certificate request and add it to the request database (using the *url* argument):

Note The request file name should have a ".req" extension and the certificate file name a ".crt" extension.

```
Router# crypto pki server mycs request pkcs10 tftp://192.0.2.129/router5
% Retrieving Base64 encoded or PEM formatted PKCS10 enrollment request...
Reading file from tftp://192.0.2.129/router5.req
Loading router5.req from 192.0.2.129 (via Ethernet0): !
[OK - 582 bytes]

% Enrollment request pending, reqId=1


Router# crypto pki server mycs grant 1
% Writing out the granted certificate...
!Writing file to tftp://192.0.2.129/router5.crt!
```

The following example shows how to manually add a hexadecimal-encoded certificate request with PEM boundaries to the request database in Cisco IOS Release 15.0(1)M and earlier:

```
Router# crypto pki server mycs request pkcs10 scep hex 0C4A3A2CA5C2E66DDCD740A4259759E2
5811E7CB133BAC936EF48C6187F4AD22 3
PKCS10 request in hex
Enter the PKCS10 in hexidecimal representation....

Router(config-pubkey)# 3082010E 3081B902 0100301D 311B3019 06092A86 4886F70D 01090216
0C697073
Router(config-pubkey)# 6563662D 33383435 61305C30 0D06092A 864886F7 0D010101 0500034B
00304802
Router(config-pubkey)# 4100B660 EF764AD6 A896E03E 0D1A1A16 5450857C 9B2CC04E B61719E5
2216CBF2
Router(config-pubkey)# 1973B464 17E78829 22CDBD87 FBD015F1 2A0A8DD7 5396EAA1 A2A65132
912466D2
Router(config-pubkey)# 62C90203 010001A0 37301406 092A8648 86F70D01 09073107 13056369
73636F30
Router(config-pubkey)# 1F060A60 86480186 F8450109 08311104 0F300D30 0B060355 1D0F0404
030205A0
Router(config-pubkey)# 300D0609 2A864886 F70D0101 04050003 410062A5 81B4C7F2 BDCEE03D
998BAD2B
Router(config-pubkey)# 1E763461 EBB812EB 4082E2BB 273AA5DD 74FF7E12 E16035E9 4525A041
AF65E48F
Router(config-pubkey)# F0E6E13C 2646F943 5C23A634 BC50BC1F 343A
Router(config-pubkey)# 30820123 3081CE02 0101300D 06092A86 4886F70D 01010405 00301D31
1B301906
Router(config-pubkey)# 092A8648 86F70D01 0902160C 69707365 63662D33 38343561 301E170D
30393031
Router(config-pubkey)# 31323032 33323039 5A170D31 39303131 30303233 3230395A 301D311B
30190609
Router(config-pubkey)# 97F8335 DDA951
Router(config-pubkey)# quit
Enter the certificate in hexidecimal representation....

Router(config-pubkey)# quit
```

The following example shows how to manually add a hexadecimal-encoded certificate request with PEM boundaries to the request database in Cisco IOS Release 15.1(1)T and later:

```
Router# crypto pki server mycs request pkcs10 scep hex 0C4A3A2CA5C2E66DDCD740A4259759E2
5811E7CB133BAC936EF48C6187F4AD22 3
PKCS10 request in hex
Enter the PKCS10 in hexidecimal representation....
```

```
Router(config-pki-hexmode)# 3082010E 3081B902 0100301D 311B3019 06092A86 4886F70D 01090216
0C697073
Router(config-pki-hexmode)# 6563662D 33383435 61305C30 0D06092A 864886F7 0D010101 0500034B
00304802
Router(config-pki-hexmode)# 4100B660 EF764AD6 A896E03E 0D1A1A16 5450857C 9B2CC04E B61719E5
2216CBF2
Router(config-pki-hexmode)# 62C90203 010001A0 37301406 092A8648 86F70D01 09073107 13056369
73636F30
Router(config-pki-hexmode)# 1F060A60 86480186 F8450109 08311104 0F300D30 0B060355 1D0F0404
030205A0
Router(config-pki-hexmode)# 300D0609 2A864886 F70D0101 04050003 410062A5 81B4C7F2 BDCEE03D
998BAD2B
Router(config-pki-hexmode)# 1E763461 EBB812EB 4082E2BB 273AA5DD 74FF7E12 E16035E9 4525A041
AF65E48F
Router(config-pki-hexmode)# F0E6E13C 2646F943 5C23A634 BC50BC1F 343A
Router(config-pki-hexmode)# 30820123 3081CE02 0101300D 06092A86 4886F70D 01010405 00301D31
1B301906
Router(config-pki-hexmode)# 092A8648 86F70D01 0902160C 69707365 63662D33 38343561 301E170D
30393031
Router(config-pki-hexmode)# 31323032 33323039 5A170D31 39303131 30303233 3230395A 301D311B
30190609
Router(config-pki-hexmode)# 2A864886 F70D0109 02160C69 70736563 662D3338 34356130 5C300D06
092A8648
Router(config-pki-hexmode)# 6F70D01 01010500 034B0030 48024100 B660EF76 4AD6A896 E03E0D1A
1A165450
Router(config-pki-hexmode)# 857C9B2C C04EB617 19E52216 CBF21973 B46417E7 882922CD BD87FBD0
15F12A0A
Router(config-pki-hexmode)# 8DD75396 EAA1A2A6 51329124 66D262C9 02030100 01300D06 092A8648
86F70D01
Router(config-pki-hexmode)# 01040500 03410041 B2EBC44A 7F5FD26A DBAAB574 655D0C5D 84CCC7B5
48643525
Router(config-pki-hexmode)# E85E4E06 5465A27F 6066BC8C 52AF9FF4 CE6A9C66 44441BF0 053325DC
736FD696
Router(config-pki-hexmode)# 97F8335 DDA951
Router(config-pki-hexmode)# quit
Enter the certificate in hexidecimal representation....

Router(config-pki-hexmode)# quit
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.
crypto pki server grant	Grants all or certain SCEP requests.
show crypto pki server	Displays the current state and configuration of a certificate server.

crypto pki server revoke

To revoke a certificate on the basis of its serial number, use the **crypto pki server revoke** command in privileged EXEC mode.

crypto pki server *cs-label* **revoke** *certificate-serial-number*

Syntax Description

cs-label	Name of the certificate server. The name must match the name specified via the **crypto pki server** command.
certificate-serial-number	Serial number of the certificate that is to be revoked. The serial number can be a hexadecimal number with the prefix "0x" (for example, 0x4c) or a decimal number (for example, 76).

Defaults

Certificates are revoked on the basis of their name.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
15.0(1)M	The command was modified to remove the serial-number check against the last-issued serial number.

Usage Guidelines

When a new certificate revocation list (CRL) is issued, the certificate server obtains the previous CRL, makes the appropriate changes, and resigns the new CRL. A new CRL is issued after a certificate is revoked from the CLI. If this process negatively affects router performance, the **crypto pki server revoke** command can be used to revoke a list or range of certificates.

Note In Cisco IOS Release 15.0(1)M, the serial number to be revoked is not compared with the last-issued serial number.

Note A new CRL cannot be issued unless the current CRL is revoked or changed.

Examples

The following examples show how to revoke a certificate with the serial number 76 (for example, 0x4c in hexidecimal) from the certificate server "mycs":

```
Router# crypto pki server mycs revoke 76
Router# crypto pki server mycs revoke 0x4c
```

Related Commands

Command	Description
cdp-url	Specifies that CDP should be used in the certificates that are issued by the certificate server.
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.

crypto pki server start

To enable a Cisco IOS certificate server, use the **crypto pki server start** command in privileged EXEC mode. To disable a certificate server, use the **crypto pki server stop** command.

crypto pki server *servername* **start**

Syntax Description

servername	Name of the certificate server. **Note** The certificate server name must not exceed 13 characters.

Command Default

The certificate server is disabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Using the **crypto pki server start** command is the same as using the **no shut** command in DSP configuration mode.

Examples

The following example shows how to enable a certificate server on a router:

```
Router# crypto pki server MYCA start
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password:

Re-enter password:

% Certificate Server enabled.
```

Related Commands

Command	Description
crypto pki server stop	Disables a Cisco IOS certificate server.
show crypto pki server	Displays the current state and configuration of a certificate server.

crypto pki server stop

To disable a Cisco IOS certificate server, use the **crypto pki server stop** command in privileged EXEC mode.

crypto pki server *servername* **stop**

Syntax Description

servername	Name of the certificate server.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Using the **crypto pki server stop** command is the same as using the **shutdown** command in DSP configuration mode.

Examples

The following example shows how to disable a certificate server:

```
Router# crypto pki server MYCA stop
Certificate server 'shut' event has been queued for processing.
```

Related Commands

Command	Description
crypto pki server start	Enables a Cisco IOS certificate server.
show crypto pki server	Displays the current state and configuration of a certificate server.

crypto pki server trim

To trim certificates from the certificate revocation list (CRL), use the **crypto pki server trim** command in privileged EXEC mode.

crypto pki server [*cs-label*] **trim** {**expired** [*start-number* [*end-number*] [**verbose**]] | **generate expired-list** [*start-number end-number*] [**url** *url*] | **url** *url* [**verbose**]}

Syntax Description

cs-label	Name of the certificate server. The name must match the name specified using the **crypto pki server** command.
expired	Specifies that the expired certificates are to be trimmed from the CRL.
start-number	The beginning of the certificate serial number range to check and trim from the CRL if the certificate has expired.
end-number	(Optional) The ending number of the certificate serial number range to check and trim from the CRL if the certificate has expired.
verbose	Displays information about the action taken on the certificates checked in the CRL.
generate	Generates information about CRL trimming.
expired-list	Generates information about trimmed expired certificates.
url *url*	Specifies the location of the expired certificate list, which contains a list of certificate serial numbers to be trimmed from the CRL.

Command Default

All certificates in the specified certificate server database will be searched to locate and to trim expired certificates.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **generate** keyword was added.

Usage Guidelines

This command trims expired certificates from the CRL. Only certificates that are expired and have accurate and complete information in the certificate database can be trimmed from the database.

Depending on the size and location of the certificate database, searching the database for expired certificates may be a time-consuming process. Depending on your environment, you may choose one of three methods to search and to trim your CRL:

- Search the entire certificate database.

  This is usually the most time-consuming and resource-consuming method.

- Specify a range of certificate serial numbers to search.

If a large number of certificates are in your certificate database or if your certificate database is stored at a remote location (for example, TFTP or Secure Copy [SCP]) you may limit the range of certificates to search by specifying both the starting and ending certificate serial numbers. If no starting and ending certificate serial numbers are specified, the entire certificate database will be searched and all expired certificates will be trimmed.

- Use an input list to specify the expired certificates to be trimmed from the CRL.

  This is the most scalable method because it divides the process into two steps: searching the certificate database for expired certificates and trimming the CRL. An input file listing expired certificate serial numbers may be generated using a Perl script or similar program, manually, or by issuing the **crypto pki server trim generate expired-list** command. The input list must follow the format as shown:

```
# CRL Trimming file generated on 01/31/2008
version=1
35
37
```

  Lines that begin with a pound sign (#) are inserted comments. The second line contains a version string indicating the file type. Each remaining line (in this example lines 35 and 37) contains a certificate serial number indicating one certificate to be removed from the CRL.

Examples

The following example shows how to check and trim the CRL of all expired certificates in the certificate database for the certificate server “mycs”:

```
Router# crypto pki server mycs trim expired
```

The following example shows how to check and trim the CRL of expired certificates within the certificate serial number range 0x1–0x3 in the certificate database for the certificate server “mycs”. The result is the same as generating and using an input file of expired certificate serial numbers, as shown in the next example.

```
Router# crypto pki server mycs trim expired 0x1 end 0x3
```

The following example shows how to generate a list of expired certificate serial numbers, store the list on an HTTP server, then use the resulting list to trim the CRL of all expired certificates for the certificate server “mycs”:

```
Router# crypto pki server mycs trim generate expired-list 0x1 0x3 url
http://databaselocation/expired-certs.1st

Router# crypto pki server mycs trim url http://databaselocation/expired-certs.1st
```

The following example shows how to check and trim the CRL for only one certificate serial number in the certificate database for the certificate server “mycs.” If the certificate with the serial number 45 has expired, it will be trimmed from the CRL.

```
Router# crypto pki server mycs trim expired 0x2
```

The following example shows how to trim the CRL of all expired certificates for the certificate server “mycs” and display the resulting action taken for each certificate serial number:

```
Router# crypto pki server mycs trim expired verbose

Certificate 2: Expired. Removed from CRL.
Certificate F4240: Expired. Removed from CRL.
```

```
Certificate 4593: Not Removed.
Certificate 1234: Not Removed.
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.
crypto pki server trim generate expired-list	Generates a list of expired certificates in the CRL.

crypto pki server trim generate expired-list

To generate a list of expired certificates in the current certificate revocation list (CRL), use the **crypto pki server trim generate expired-list** command in privileged EXEC mode.

crypto pki server *cs-label* **trim generate expired-list** [**start** *number* **end** *number*] [**url** *url*]

Syntax Description

cs-label	Name of the certificate server. The name must match the name specified via the **crypto pki server** command.
start *number*	(Optional) The first certificate serial number from which to begin searching the CRL for expired certificates. To locate expired certificates within a range *both* the starting certificate serial number and the ending certificate serial number must be specified.
end *number*	(Optional) The last certificate serial number that will be checked when searching the CRL for a range of expired certificates.
url *url*	(Optional) Specifies the location where the resulting list of expired certificates will be stored.

Command Default

All certificates in the specified certificate server database will be searched to locate expired certificates.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

This command generates a list of expired certificates that are in the CRL for the specified certificate server. The resulting list of expired certificates may be used as input to the **crypto pki server trim** command to remove the listed certificates from the CRL resulting in trimming, or revoking, the expired certificates.

Only certificates that have accurate and complete information in the certificate database can be automatically added to the list of expired certificates and later trimmed from the database. Only CRL entries for expired certificates can be trimmed.

If there are a large number of certificates in your certificate database or if your certificate database is stored at a remote location, for example TFTP or SCP, you may limit the range of certificates to search by specifying *both* the starting and ending certificate serial numbers. If no starting and ending certificate serial numbers are specified, the entire certificate database will be searched and all expired certificates will be added to the expired certificates list.

A URL may be specified to save the list of expired certificates to a specified location. If no URL is specified, the list of expired certificates will be printed on your terminal. The list may then be cut and pasted to a file.

Examples

The following example shows both how to generate a list of expired certificates within the certificate serial number range 34–38 in the certificate database for the certificate server "mycs" and how to save the resulting list to an HTTP location:

```
Router# crypto pki server mycs trim generate expired-list start 34 end 38 url
http://databaselocation/expired-certs.1st
```

The following example shows the resulting list of expired certificates in the file expired-certs.1st:

```
# CRL Trimming file generated on 01/31/2008
version=1
35
37
```

Lines that begin with a pound sign (#) are inserted comments. The second line contains a version string indicating the file type. Each remaining line, in this example lines 35 and 37, contains a certificate serial number indicating one certificate to be removed from the CRL.

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.
crypto pki server trim	Trims certificates from the certificate revocation list.

crypto pki server unrevoke

To recover a revoked certificate, that is to remove a certificate from the certificate revocation list (CRL), use the **crypto pki server unrevoke** command in privileged EXEC mode.

crypto pki server *cs-label* **unrevoke** *certificate-serial-number*

Syntax Descriptions

cs-label	Name of the certificate server. The name must match the name specified via the **crypto pki server** command.
certificate-serial-number	Serial number of the certificate that is to be recovered. The serial number can be a hexadecimal number with the prefix "0x" (for example, 0x4c) or a decimal number (for example, 76).

Command Default

None.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

If a certificate is erroneously revoked, either the client has to reenroll in the PKI or the administrator may recover the revoked certificate by issuing the **crypto pki server unrevoke** command. This command removes a certificate, specified by its serial number, from the CRL. The CRL is then resigned and can be republished.

Examples

The following examples show how to unrevoke a certificate with the serial number 76, or 0x4c in hexidecimal, from the certificate server "mycs":

```
Router# crypto pki server mycs unrevoke 76
Router# crypto pki server mycs unrevoke 0x4c
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.
cyrpto pki server revoke	Revokes a certificate based on its serial number.

crypto pki token change-pin

To change the user PIN on the USB eToken, use the **crypto pki token change-pin** command in privileged EXEC mode.

crypto pki token *token-name* [**admin**] **change-pin** [*pin*]

Syntax Description

token-name	Name of USB token specified via the **crypto pki token login** command.
admin	(Optional) The router will change the administrative PIN on the USB token. If this keyword is not issued, the router will change the user pin.
pin	(Optional) User PIN required to access the etoken.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.

Usage Guidelines

If you want to change the administrative PIN on the token, you must be logged into the eToken as an admin via the **crypto pki token admin login** command.

After the user PIN has been changed, you must reset the login failure count to zero (via the **crypto pki token max-retries** command). The maximum number of allowable login failures is set (by default) to 15.

Examples

The following example shows that the user PIN was changed to 1234:

```
crypto pki token usbtoken0 admin login 5678
crypto pki token usbtoken0 change-pin 1234
```

Related Commands

Command	Description
crypto pki token login	Logs into the USB eToken.
crypto pki token max-retries	Sets the maximum number of allowed failed login attempts.

crypto pki token encrypted-user-pin

To encrypt a USB token PIN that is stored in private NVRAM, use the **crypto pki token encrypted-user-pin** command in global configuration mode. To decrypt the token's PIN, use the **no** form of this command.

crypto pki token {*token-name* | **default**} **encrypted-user-pin** [**write**] [**passphrase** *passphrase*]

no crypto pki token {*token-name* | **default**} **encrypted-user-pin** [**write**] [**passphrase** *passphrase*]

Syntax Description

token-name	Name of the token that will have its PIN encrypted.
default	Configures default values for tokens.
write	(Optional) Writes to memory immediately after the passphrase is entered. This keyword saves the running configuration to NVRAM.
passphrase *passphrase*	(Optional) Enables noninteractive command-line interface (CLI). If you do not issue this keyword, you will automatically be prompted for the passphrase. **Tip** Noninteractive CLI is provided for instances where users will not be responding to prompts, for example in scripts, configuration tools, or other automated processes. If you are issuing this command from the console, it is recommended that you use the interactive CLI to help protect against observation from unauthorized persons.

Command Default

The PIN stored in private NVRAM is not encrypted.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.4(11)T	This command was integrated into the Cisco IOS Release 12.4(11)T and implemented on 7200VXR NPE-G2 platform.
15.0(1)M	This command was modified earlier than Cisco IOS Release 15.0(1)M. The **default** keyword was added.

Usage Guidelines

After the token's PIN is encrypted with the **crypto pki token encrypted-user-pin** command, no action is taken when you insert the token into the router. The user must log in to the router and enter the passphrase to decrypt the PIN before the router can use the PIN to log in to the token.

After the PIN has been successfully decrypted, the router will execute the configuration commands from the token at privilege level 15.

Tip It is recommended that you create a passphrase different from the token's PIN.

Also, the user should log in to the token as a "normal user" (a privilege level 1 user), so the user cannot access commands that can alter the configuration of the router.

Examples

The following example shows the configuration of a user PIN and the encryption of that user PIN:

```
! Configure the user PIN.
Router(config)# crypto pki token usbtoken0: user-pin
Enter password:
!
! Now, the user PIN can be encrypted.
!
Router(config)# crypto pki token usbtoken0: encrypted-user-pin
 Enter passphrase:
Router(config)# exit
Router#
Router# show running config
.
.
.
     crypto pki token usbtoken0 user-pin *encrypted*
.
.
.
```

Related Commands

Command	Description
crypto pki token user-pin	Creates a PIN that automatically allows the router to log in to the USB token at router startup.
privilege	Configures a new privilege level for users and associates commands with that privilege level.

crypto pki token label

To set or change the name of a USB token label, use the **crypto pki token label** command in global configuration mode.

crypto pki token *device*: **label** *token-label*

Syntax Description

device:	Location or name of the USB device.
token-label	Specifies the label, or name, of the USB token. • *token-label* may be up to 31 alphanumeric characters in length, including dashes and underscores.

Command Default

No label is set. The USB token is known by its factory name.

Command Modes

Global configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.

Usage Guidelines

After you have logged in your USB token to the router, you may want to change the factory default label. Changing the default factory name to a unique name is useful when configuring multiple USB tokens for automatic login, secondary configuration files, or other token specific settings.

Note Either the device name or label may be used to specify the USB token.

If using the device name, it is followed by a colon, ":".

Examples

The following example shows how to change the USB token label from the "oldlabel" to "newlabel" after the token has been logged in. The router will not use the "newlabel" until the next time the token is inserted or the router is reloaded:

```
Router#
Router# configure terminal
Router(config)# crypto pki token oldlabel label newlabel
  Token label changed.
```

Related Commands

Command	Description
crypto pki token user-pin	Creates a PIN that automatically allows the router to log into the USB token at router startup.

crypto pki token lock

To lock the token, use the **crypto pki token lock** command in privileged EXEC mode.

crypto pki token *token-name* **lock** [**user-pin**] [**passphrase** *passphrase*]

Syntax Description

token-name	Name of the token that is to be locked.
user-pin	(Optional) Specifies the USB token PIN if set.
passphrase *passphrase*	(Optional) Enables the noninteractive command-line interface (CLI). If you do not issue this keyword, you will automatically be prompted for the passphrase. **Tip** The noninteractive CLI is provided for instances where users will not be responding to prompts, for example in scripts, configuration tools, or other automated processes. If you are issuing this command from the console, it is recommended that you use the interactive CLI to help protect against observation from unauthorized persons.

Command Default

The token is not locked.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.

Usage Guidelines

After you have locked a token with the **crypto pki token lock** command, all Rivest, Shamir, and Adelman (RSA) keys that have been loaded from the token will be deleted and, if configured, the secondary "unconfig" file will run with full privileges.

Examples

The following example shows how to reload a router, unlock the PIN, and then lock the PIN again:

```
Router> enable
 Password:
Router# crypto pki token usbtoken0: unlock
 Token eToken is usbtoken0
!
Enter passphrase:
Token login to usbtoken0(eToken) successful
Router#
Sep 20 22:31:13.128: %CRYPTO-6-TOKENLOGIN: Cryptographic Token eToken
Login Successful
```

```
Router# crypto pki token usbtoken0: lock
```

Related Commands

Command	Description
crypto pki token name secondary unconfig file	Specifies a secondary “unconfig” file.
crypto pki token unlock	Unlocks the token and decrypts the PIN that is stored in private NVRAM.

crypto pki token login

To log into the USB eToken, use the **crypto pki token login** command in privileged EXEC mode.

crypto pki token *token-name* [**admin**] **login** [*pin*]

Syntax Description

token-name	Name of USB eToken.
admin	(Optional) The router will attempt to log into the token as an administrator. If this keyword is not issued, the router will attempt to log into the token as a user. **Note** If you want to change the PIN via the **crypto pki token change-pin** command, you must issue this keyword.
pin	(Optional) User PIN required to access the token. If a user PIN is not specified, the default PIN, 1234567890, is used.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.

Usage Guidelines

This command allows you to manually log into a USB eToken. To automatically log into an eToken, issue the **crypto pki token user-pin** command, which allows you to create a PIN for automatic login.

Examples

The following example shows how to log into the USB eToken manually:

```
crypto pki token usbtoken0:login 1234567890
```

Related Commands

Command	Description
crypto pki token logout	Logs the router out of the USB eToken.

crypto pki token logout

To log the router out of the USB eToken, use the **crypto pki token logout** command in privileged EXEC mode.

crypto pki token *token-name* **logout**

Syntax Description

token-name	Name of USB eToken specified via the **crypto pki token login** command.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.

Usage Guidelines

If you want to save any data to the USB eToken, you must log back into the eToken.

Examples

The following example shows how to successfully log out of a USB eToken:

```
crypto pki token usbtoken0:logout
Token eToken is usbtoken0

Token logout from usbtoken0(eToken) successful
*Jan 28 05:46:59.544:%CRYPTO-6-TOKENLOGOUT:Cryptographic Token eToken Logout Successful
```

Related Commands

Command	Description
crypto pki token login	Logs into the USB eToken.

crypto pki token max-retries

To set the maximum number of allowed failed login attempts, use the **crypto pki token max-retries** command in global configuration mode. To return to the default functionality (which is 15 failed login attempts), use the **no** form of this command.

crypto pki token {*token-name* | **default**} **max-retries** [*number*]

no crypto pki token {*token-name* | **default**} **max-retries** [*number*]

Syntax Description

token-name	Name of USB token that the router will log into.
default	Default value is to be used.
number	(Optional) Number of consecutive failed login attempts the router will allow before locking out the user. Available range: 0 to 15. Default value is 15.

Defaults

15 failed login attempts are allowed

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.

Usage Guidelines

After the user PIN is changed via the **crypto pki token change-pin command**, the login failure count is automatically reset to 15; however, it is recommended that the login failure count be set to zero.

Examples

The following example shows how to change the allowed maximum number of failed login attempts to 20:

```
crypto pki token usbtoken0 max-retries 20
```

Related Commands

Command	Description
crypto pki token change-pin	Changes the user PIN number on the USB eToken.
crypto pki token login	Logs into the USB eToken.

crypto pki token removal timeout

To set the time interval that the router waits before removing the Rivest, Shamir, and Adelman (RSA) keys that are stored in the eToken, use the **crypto pki token removal timeout** command in global configuration mode. To return to the default functionality (which is no timeout), use the **no** form of this command.

crypto pki token {*token-name* | **default**} **removal timeout** [*seconds*]

no crypto pki token {*token-name* | **default**} **removal timeout** [*seconds*]

Syntax Description

token-name	Name of USB eToken that is being removed from the router.
default	Default value, which is automatic RSA key removal, is to be used.
seconds	(Optional) Time interval, in seconds, that the router waits before removing the RSA keys and tearing down IP Security (IPSec) tunnels associated with the specified eToken. Available range: 0 to 480. **Note** If a time interval is not specified, all RSA keys and associated tunnels are immediately torn down after the eToken is removed from the router.

Defaults

The default timeout is zero, which causes the RSA keys to be removed automatically after the eToken is removed from the router. The default appears in the running configuration as:

```
crypto pki token default removal timeout 0
```

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.

Usage Guidelines

After the eToken is removed from the router, you can clear from your router any RSA keys that were obtained from the eToken; all IPSec tunnels that used those RSA keys for authentication are also torn down. Both the keys and tunnels are immediately cleared unless otherwise specified via the **crypto pki token removal timeout** command.

Although the RSA keys remain on the eToken, they can only be accessed with the correct PIN. Too many unsuccessful attempts to log into the eToken will disable the PIN and any further login attempts will be refused.

Note The **no** version of this command does not remove RSA keys from the router. To immediately remove RSA keys from the router, set the timeout value to zero.

Examples

The following example shows how to set the time that the router will wait before removing the RSA keys that are stored in the eToken after the eToken has been removed from the router:

```
crypto pki token usbtoken0 removal timeout 60
```

Related Commands

Command	Description
crypto pki token logout	Logs the router out of the USB token.
crypto pki token max-retries	Sets the maximum number of allowed failed login attempts.

crypto pki token secondary config

To merge a specified file with the running configuration after the eToken is logged in to the router, use the **crypto pki token secondary config** command in global configuration mode. To remove the specified file, use **no** form of the command.

crypto pki token {*token-name* | **default**} **secondary config** [*file*]

no crypto pki token {*token-name* | **default**} **secondary config** [*file*]

Syntax Description

token-name	Name of USB eToken that will have its running configuration merged with the secondary configuration file.
default	Sets the default values for tokens.
file	(Optional) Name of the file that will be merged with the running configuration. **Note** The filename is relative to the eToken, so the name should not include a device name such as "usbtoken0:."

Command Default

A secondary configuration file does not exist.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.
15.0(1)M	This command was modified earlier than Cisco IOS Release 15.0(1)M. The **default** keyword was added.

Usage Guidelines

Use the **crypto pki token secondary config** command if you want to merge, not overwrite, a file with the running configuration on the router. The secondary configuration is processed after the eToken is logged in to the router.

Examples

The following example shows how to merge the secondary configuration file "CONFIG1.CFG" with the current running configuration:

```
Router# configure terminal
Router(config)# crypto pki token default secondary config CONFIG1.CFG
```

Related Commands

Command	Description
crypto pki token login	Logs in to the USB eToken.
crypto pki token user-pin	Creates a PIN that automatically allows the router to log into the USB eToken at router startup.

crypto pki token secondary unconfig

To specify a secondary "unconfig" file and its location for a USB token, use the **crypto pki token secondary unconfig** command in global configuration mode. To remove secondary configuration elements from the running configuration, use the **no** form of this command.

crypto pki token {*token-name* | **default**} **secondary unconfig** [*file*]

no crypto pki token {*token-name* | **default**} **secondary unconfig** [*file*]

Syntax Description

token-name	Name of the token that is to be unlocked.
default	Configures default values for tokens.
file	(Optional) Name and location of the secondary configuration file.

Command Default

Secondary "unconfig" file will not be processed.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.
15.0(1)M	This command was modified earlier than Cisco IOS Release 15.0(1)M. The **default** keyword was added.

Usage Guidelines

Configuration files that exist on a USB token are called secondary configuration files. If you create and configure a secondary configuration file, it is executed after the token is logged in. The existence of a secondary configuration file is determined by the presence of a secondary configuration file option in the Cisco IOS configuration stored in NVRAM.

When the token is removed, logged out, or the removal timer (if set) expires, a separate "unconfig" file is processed to remove all secondary configuration elements from the running configuration. Secondary configuration and secondary "unconfig" files are executed at privilege level 15 and are not dependent on the level of the user logged in.

Examples

The following example shows a how a secondary "unconfig" file might be used to remove secondary configuration elements from the running config. For example, a secondary configuration file might be used to set up a public key infrastructure (PKI) trustpoint. A corresponding "unconfig" file, named mysecondaryunconfigfile.cfg, might contain the following command:

```
no crypto pki trustpoint token-tp
```

If the token were removed and the following commands executed, the trustpoint and associated certificates would be removed from the router's running configuration:

```
Router# configure terminal
Router(config)# no crypto pki token mytoken secondary unconfig mysecondaryunconfigfile.cfg
```

Related Commands

Command	Description
crypto pki token secondary config	Merges a specified secondary configuration file with the running configuration after the USB token is logged in to the router.
crypto pki token user-pin	Creates a PIN that automatically allows the router to log in to the USB token at router startup.

crypto pki token unlock

To unlock the token and decrypt the PIN that is stored in private NVRAM, use the **crypto pki token unlock** command in privileged EXEC mode.

crypto pki token *token-name* **unlock** [**user-pin**] [**passphrase** *passphrase*]

Syntax Description

token-name	Name of the token that is to be unlocked.
user-pin	(Optional) Specifies the USB token PIN if set.
passphrase *passphrase*	(Optional) Enables the noninteractive command-line interface (CLI). If you do not issue this keyword, you will automatically be prompted for the passphrase. **Tip** The noninteractive CLI is provided for instances where users will not be responding to prompts, for example in scripts, configuration tools, or other automated processes. **Note** If you are issuing this command from the console, it is recommended that you use the interactive CLI to help protect against observation from unauthorized persons.

Command Default

USB token is not unlocked, or decrypted.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.

Usage Guidelines

After you unlock a token via the **crypto pki token unlock** command, the Cisco IOS software will treat the token as if it is automatically logged into the router. Any Rivest, Shamir, and Adelman (RSA) keys on the token are loaded onto the router and the secondary configuration file on the token is executed (if a secondary configuration file has been configured by the user). Secondary configuration files are executed with full user privileges.

Examples

The following example shows the configuration and encryption of a user PIN and then that the router is reloading and the user PIN is being unlocked.

```
! Configuring the user PIN

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# crypto pki token usbtoken0: user-pin
     Enter password:
```

```
! Encrypt the user PIN

Router (config)# crypto pki token usbtoken0: encrypted-user-pin
     Enter passphrase:
Router(config)# exit
Router#
Sep 20 21:51:38.076: %SYS-5-CONFIG_I: Configured from console by console
!

Router# show running-config
.
.
.
crypto pki token usbtoken0 user-pin *encrypted*
.
.
.

! Reloading the router.
!
Router> enable
 Password:
!
! Decrypting the user pin.
!
Router# crypto pki token usbtoken0: unlock
 Token eToken is usbtoken0
!
Enter passphrase:
Token login to usbtoken0(eToken) successful
Router#
Sep 20 22:31:13.128: %CRYPTO-6-TOKENLOGIN: Cryptographic Token eToken
Login Successful
```

Related Commands

Command	Description
crypto pki token user-pin	Creates a PIN that automatically allows the router to log into the USB token at router startup.

crypto pki token user-pin

To create a PIN that automatically allows the router to log in to the USB eToken at router startup, use the **crypto pki token user-pin** command in global configuration mode. To remove the stored PIN from the configuration, use the **no** form of this command.

crypto pki token {*token-name* | **default**} **user-pin** [*pin*] [*token-pin*]

no crypto pki token {*token-name* | **default**} **user-pin** [*pin*] [*token-pin*]

Syntax Description

token-name	Name of USB eToken that the router will log in to.
default	Sets the default values for tokens.
user-pin	Specifies the PIN to access token.
pin	(Optional) User PIN required to log in to the eToken. The PINs are stored in private NVRAM. If a user PIN is not specified, the default PIN, 1234567890, will be used.
token-pin	(Optional) Token PIN name.

Command Default

If this command is not issued, the router cannot access the eToken.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.
15.0(1)M	This command was modified earlier than Cisco IOS Release 15.0(1)M. The **default** keyword was added.

Usage Guidelines

After the eToken is plugged into the router, the router will use the specified PIN (or the default PIN if no PIN is specified) to automatically log in as the user.

Examples

The following example shows how to access the eToken via the user PIN “12345”:

```
crypto pki token usbtoken0 user-pin 12345
```

Related Commands

Command	Description
crypto pki login	Logs in to the USB eToken.
crypto pki token logout	Logs the router out of the USB eToken.

crypto pki trustpoint

To declare the trustpoint that your router should use, use the **crypto pki trustpoint** command in global configuration mode. To delete all identity information and certificates associated with the trustpoint, use the **no** form of this command.

crypto pki trustpoint *name* **redundancy**

no crypto pki trustpoint *name*

Syntax Description

name	Creates a name for the trustpoint. (If you previously declared the trustpoint and just want to update its characteristics, specify the name you previously created.)
redundancy	(Optional) Specifies that the key, and any certificates associated with it, should be synchronized to the standby certificate authority (CA).

Defaults

Your router does not recognize any trustpoints until you declare a trustpoint using this command.

Your router uses unique identifiers during communication with Online Certificate Status Protocol (OCSP) servers, as configured in your network.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	The **crypto ca trustpoint** command was added.
12.2(15)T	The **match certificate** subcommand was introduced.
12.3(7)T	This command replaced the **crypto ca trustpoint** command. You can still enter the **crypto ca trusted-root** or **crypto ca trustpoint** command, but the command will be written in the configuration as "crypto pki trustpoint."
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.3(14)T	The **enrollment selfsigned** subcommand was introduced.
12.4(4)T	The **ocsp disable-nonce** subcommand was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)M	This command was modified. The **redundancy** keyword was introduced.

Usage Guidelines

Declaring Truspoints

Use the **crypto pki trustpoint** command to declare a trustpoint, which can be a self-signed root certificate authority (CA) or a subordinate CA. Issuing the **crypto pki trustpoint** command puts you in ca-trustpoint configuration mode.

You can specify characteristics for the trustpoint using the following subcommands:

- **crl**—Queries the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked.

- **default (ca-trustpoint)**—Resets the value of ca-trustpoint configuration mode subcommands to their defaults.
- **enrollment**—Specifies enrollment parameters (optional).
- **enrollment http-proxy**—Accesses the CA by HTTP through the proxy server.
- **enrollment selfsigned**—Specifies self-signed enrollment (optional).
- **match certificate**—Associates a certificate-based access control list (ACL) defined with the **crypto ca certificate map** command.
- **ocsp disable-nonce**—Specifies that your router will not send unique identifiers, or nonces, during OCSP communications
- **primary**—Assigns a specified trustpoint as the primary trustpoint of the router.
- **root**—Defines the TFTP to get the CA certificate and specifies both a name for the server and a name for the file that will store the CA certificate.

Specifying Use of Unique Identifiers

When using OCSP as your revocation method, unique identifiers, or nonces, are sent by default during peer communications with the OCSP server. The use of unique identifiers during OCSP server communications enables more secure and reliable communications. However, not all OCSP servers support the use of unique dentures, see your OCSP manual for more information. To disable the use of unique identifiers during OCSP communications, use the **ocsp disable-nonce** subcommand.

Examples

The following example shows how to declare the CA named *ka* and specify enrollment and CRL parameters:

```
crypto pki trustpoint ka
 enrollment url http://kahului:80
```

The following example shows a certificate-based ACL with the label Group defined in a **crypto pki certificate map** command and included in the **match certificate** subcommand of the **crypto pki trustpoint** command:

```
crypto pki certificate map Group 10
 subject-name co ou=WAN
 subject-name co o=Cisco
!
crypto pki trustpoint pki1
 match certificate Group
```

The following example shows a self-signed certificate being designated for a trustpoint named local using the **enrollment selfsigned** subcommand of the **crypto pki trustpoint** command:

```
crypto pki trustpoint local
 enrollment selfsigned
```

The following example shows the unique identifier being disabled for OCSP communications for a previously created trustpoint named *ts*:

```
crypto pki trustpoint ts
 ocsp disable-nonce
```

The following example shows the **redundancy** keyword specified in the **crypto pki trustpoint** command:

```
Router(config)#crypto pki trustpoint mytp
Router(ca-trustpoint)#redundancy
Router(ca-trustpoint)#show
```

```
 redundancy
 revocation-check crl
end
```

Related Commands

Command	Description
crl	Queries the CRL to ensure that the certificate of the peer has not been revoked.
default (ca-trustpoint)	Resets the value of a ca-trustpoint configuration subcommand to its default.
enrollment	Specifies the enrollment parameters of your CA.
enrollment http-proxy	Accesses the CA by HTTP through the proxy server.
primary	Assigns a specified trustpoint as the primary trustpoint of the router.
root	Obtains the CA certificate via TFTP.

crypto provisioning petitioner

To configure a device to become an easy secure device provisioning (SDP) petitioner and enter tti-petitioner configuration mode, use the **crypto provisioning petitioner** command in global configuration mode. To disable petitioner support, use the **no** form of this command.

crypto provisioning petitioner

no crypto provisioning petitioner

Syntax Description

This command has no arguments or keywords.

Defaults

A device (with a crypto image) is configured to be an SDP petitioner.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	The **crypto wui tti petitioner** command was introduced.
12.3(14)T	This command replaced the **crypto wui tti petitioner** command.

Usage Guidelines

SDP uses Trusted Transitive Introduction (TTI) to easily deploy public key infrastructure (PKI) between two end devices. TTI, which is a communication protocol that provides a bidirectional introduction between two end entities, involves the following three entities:

- Introducer—A mutually trusted device that introduces the petitioner to the registrar. The introducer can be a device user, such as a system administrator.
- Petitioner—A new device that is joined to the secure domain.
- Registrar—A server that authorizes the petitioner. The registrar can be a certificate server.

Note Because the petitioner is enabled by default on the device, you only have to issue the **crypto provisioning petitioner** command if you have previously disabled the petitioner or if you want to use an existing trustpoint instead of the automatically generated trustpoint.

Examples

After the SDP exchange is complete, the petitioner will automatically enroll with the registrar and obtain a certificate. The following sample output from the **show running-config** command shows an automatically generated configuration at the petitioner.

Note The petitioner will not have any TTI-specific configuration in the beginning except that the IP HTTP server will be turned on and the Domain Name System (DNS) server needs to be properly configured.)

```
crypto pki trustpoint tti
! Enrollment url contains the registrar CS details
 enrollment url http://pki1-36a.cisco.com:80
 revocation-check crl
 rsakeypair tti 1024
 auto-enroll 70
```

Related Commands

Command	Description
crypto provisioning registrar	Configures a device to become an SDP registrar and enters tti-registrar configuration mode.
trustpoint (tti-petitioner)	Specifies the trustpoint that is to be associated with the TTI exchange between the SDP petitioner and the SDP registrar.

crypto provisioning registrar

To configure a device to become an easy secure device provisioning (SDP) registrar and enter tti-registrar configuration mode, use the **crypto provisioning registrar** command in global configuration mode. To disable registrar support, use the **no** form of this command.

crypto provisioning registrar

no crypto provisioning registrar

Syntax Description

This command has no arguments or keywords.

Defaults

The registrar is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	The **crypto wui tti registrar** command was introduced.
12.3(14)T	This command replaced the **crypto wui tti registrar** command.

Usage Guidelines

SDP uses Trusted Transitive Introduction (TTI) to easily deploy public key infrastructure (PKI) between two end devices. TTI, which is a communication protocol that provides a bidirectional introduction between two end entities, involves the following three entities:

- Introducer—A mutually trusted device that introduces the petitioner to the registrar. The introducer can be a device user, such as a system administrator.
- Petitioner—A new device that is joined to the secure domain.
- Registrar—A server that authorizes the petitioner.

Although any device that contains a crypto image can be the registrar, it is recommended that the registrar be either a Cisco IOS certificate server registration authority (RA) or a Cisco IOS certificate server root.

Examples

The following sample output from the **show running-config** command verifies that the certificate server "cs1" was configured and associated with the TTI exchange between the registrar and petitioner:

```
crypto pki server cs1
 issuer-name CN = ioscs,L = Santa Cruz,C =US
 lifetime crl 336
 lifetime certificate 730
!
crypto pki trustpoint pki-36a
 enrollment url http://pki-36a:80
 ip-address FastEthernet0/0
 revocation-check none
!
```

```
crypto pki trustpoint cs1
 revocation-check crl
 rsakeypair cs1
!
!
crypto pki certificate chain pki-36a
 certificate 03
  308201D0 30820139 A0030201 02020103 300D0609 2A864886 F70D0101 04050030
  34310B30 09060355 04061302 55533114 30120603 55040713 0B205361 6E746120
  4372757A 310F300D 06035504 03130620 696F7363 73301E17 0D303430 31333130
  39333334 345A170D 30363031 33303039 33333434 5A303A31 38301606 092A8648
  86F70D01 09081309 31302E32 332E322E 32301E06 092A8648 86F70D01 09021611
  706B692D 3336612E 63697363 6F2E636F 6D305C30 0D06092A 864886F7 0D010101
  0500034B 00304802 4100AFFA 8F429618 112FAB9D 01F3352E 59DD3D2D AE67E31D
  370AC4DA 619735DF 9CF4EA13 64E4B563 C239C5F0 1578B773 07BED641 A18CA629
  191884B5 61B66ECF 4D110203 010001A3 30302E30 0B060355 1D0F0404 030205A0
  301F0603 551D2304 18301680 141DA8B1 71652961 3F7D69F0 02903AC3 2BADB137
  C6300D06 092A8648 86F70D01 01040500 03818100 67BAE186 327CED31 D642CB39
  AD585731 95868683 B950DF14 3BCB155A 2B63CFAD B34B579C 79128AD9 296922E9
  4DEDFCAF A7B5A412 AB1FC081 09951CE3 08BFFDD9 9FB1B9DA E9AA42C8 D1049268
  C524E58F 11C6BA7F C750320C 03DFB6D4 CBB3E739 C8C76359 CE939A97 B51B3F7F
  3FF;A9D82 9CFDB6CF E2503A14 36D0A236 A1CCFEAE
  quit
 certificate ca 01
  30820241 308201AA A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  34310B30 09060355 04061302 55533114 30120603 55040713 0B205361 6E746120
  4372757A 310F300D 06035504 03130620 696F7363 73301E17 0D303430 31333130
  39333132 315A170D 30373031 33303039 33313231 5A303431 0B300906 03550406
  13025553 31143012 06035504 07130B20 53616E74 61204372 757A310F 300D0603
  55040313 0620696F 73637330 819F300D 06092A86 4886F70D 01010105 0003818D
  00308189 02818100 FC0695AF 181CE90A 1B34B348 BA957178 680C8B51 07802AC3
  BF77B9C6 CB45092E 3C22292D C7D5FFC1 899185A1 FD8F37D5 C44FC206 6D1FA581
  E2264C83 1CC7453E 548C89C6 F3CD25BC 9BFFE7C5 E6653A06 62133950 78BED51B
  49128428 AB237F80 83A530EA 6F896193 F2134B54 D181F059 348AA84B 21EE6D80
  727BF668 EB004341 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
  01FF300E 0603551D 0F0101FF 04040302 0186301D 0603551D 0E041604 141DA8B1
  71652961 3F7D69F0 02903AC3 2BADB137 C6301F06 03551D23 04183016 80141DA8
  B1716529 613F7D69 F002903A C32BADB1 37C6300D 06092A86 4886F70D 01010405
  00038181 00885895 A0141169 3D754EB2 E6FEC293 5BF0A80B E424AA2F A3F59765
  3463AAD1 55E71F0F B5D1A35B 9EA79DAC DDB40721 1344C01E 015BAB73 1E148E03
  9DD01431 A5E2887B 4AEC8EF4 48ACDB66 A6F9401E 8F7CA588 8A4199BB F8A437A0
  F25064E7 112805D3 074A154F 650D09B9 8FA19347 ED359EAD 4181D9ED 0C667C10
  8A7BCFB0 FB
  quit
crypto pki certificate chain cs1
 certificate ca 01
  30820241 308201AA A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  34310B30 09060355 04061302 55533114 30120603 55040713 0B205361 6E746120
  4372757A 310F300D 06035504 03130620 696F7363 73301E17 0D303430 31333130
  39333132 315A170D 30373031 33303039 33313231 5A303431 0B300906 03550406
  13025553 31143012 06035504 07130B20 53616E74 61204372 757A310F 300D0603
  55040313 0620696F 73637330 819F300D 06092A86 4886F70D 01010105 0003818D
  00308189 02818100 FC0695AF 181CE90A 1B34B348 BA957178 680C8B51 07802AC3
  BF77B9C6 CB45092E 3C22292D C7D5FFC1 899185A1 FD8F37D5 C44FC206 6D1FA581
  E2264C83 1CC7453E 548C89C6 F3CD25BC 9BFFE7C5 E6653A06 62133950 78BED51B
  49128428 AB237F80 83A530EA 6F896193 F2134B54 D181F059 348AA84B 21EE6D80
  727BF668 EB004341 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
  01FF300E 0603551D 0F0101FF 04040302 0186301D 0603551D 0E041604 141DA8B1
  71652961 3F7D69F0 02903AC3 2BADB137 C6301F06 03551D23 04183016 80141DA8
  B1716529 613F7D69 F002903A C32BADB1 37C6300D 06092A86 4886F70D 01010405
  00038181 00885895 A0141169 3D754EB2 E6FEC293 5BF0A80B E424AA2F A3F59765
  3463AAD1 55E71F0F B5D1A35B 9EA79DAC DDB40721 1344C01E 015BAB73 1E148E03
  9DD01431 A5E2887B 4AEC8EF4 48ACDB66 A6F9401E 8F7CA588 8A4199BB F8A437A02;
  F25064E7 112805D3 074A154F 650D09B9 8FA19347 ED359EAD 4181D9ED 0C667C10
```

```
  8A7BCFB0 FB
  quit
!
crypto provisioning registrar
 pki-server cs1
!
!
!
crypto isakmp policy 1
 hash md5
!
!
crypto ipsec transform-set test_transformset esp-3des
!
crypto map test_cryptomap 10 ipsec-isakmp
 set peer 10.23.1.10
 set security-association lifetime seconds 1800
 set transform-set test_transformset
 match address 170
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.
crypto provisioning petitioner	Configures a device to become an SDP petitioner and enters tti-petitioner configuration mode.

crypto wui tti petitioner

Note This command was replaced by the **crypto provisioning petitioner** command effective with Cisco IOS Release 12.3(14)T.

To configure a device to become an easy secure device deployment (EzSDD) petitioner and enter tti-petitioner configuration mode, use the **crypto wui tti petitioner** command in global configuration mode. To disable petitioner support, use the **no** form of this command.

crypto wui tti petitioner

no crypto wui tti petitioner

Syntax Description

This command has no arguments or keywords.

Defaults

A device (with a crypto image) is configured to be an EzSDD petitioner.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

EzSDD uses Trusted Transitive Introduction (TTI) to easily deploy public key infrastructure (PKI) between two end devices. TTI, which is a communication protocol that provides a bidirectional introduction between two end entities, involves the following three entities:

- Introducer—A mutually trusted device that introduces the petitioner to the registrar. The introducer can be a device user, such as a system administrator.
- Petitioner—A new device that is joined to the secure domain.
- Registrar—A server that authorizes the petitioner. The registrar can be a certificate server.

Note Because the petitioner is enabled by default on the device, you only have to issue the **crypto wui tti petitioner** command if you have previously disabled the petitioner or if you want to use an existing trustpoint instead of the automatically generated trustpoint.

Examples

After the EzSDD exchange is complete, the petitioner will automatically enroll with the registrar and obtain a certificate. The following sample output from the **show running-config** command shows an automatically generated configuration at the petitioner. (Note that petitioner will not have any TTI-specific configuration in the beginning except that the http server will be turned on and the Domain Name System (DNS) server needs to be properly configured.)

```
crypto pki trustpoint tti
! Enrollment url contains the registrar CS details
 enrollment url http://pki1-36a.cisco.com:80
 revocation-check crl
 rsakeypair tti 1024
 auto-enroll 70
```

Related Commands

Command	Description
crypto wui tti registrar	Configures a device to become an EzSDD registrar and enters tti-registrar configuration mode.
trustpoint (tti-petitioner)	Specifies the trustpoint that is to be associated with the TTI exchange between the EzSDD petitioner and the EzSDD registrar.

crypto wui tti registrar

Note This command was replaced by the **crypto provisioning registrar** command effective with Cisco IOS Release 12.3(14)T.

To configure a device to become an easy secure device deployment (EzSDD) registrar and enter tti-registrar configuration mode, use the **crypto wui tti registrar** command in global configuration mode. To disable registrar support, use the **no** form of this command.

crypto wui tti registrar

no crypto wui tti registrar

Syntax Description

This command has no arguments or keywords.

Defaults

The registrar is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

EzSDD uses Trusted Transitive Introduction (TTI) to easily deploy public key infrastructure (PKI) between two end devices. TTI, which is a communication protocol that provides a bidirectional introduction between two end entities, involves the following three entities:

- Introducer—A mutually trusted device that introduces the petitioner to the registrar. The introducer can be a device user, such as a system administrator.
- Petitioner—A new device that is joined to the secure domain.
- Registrar—A server that authorizes the petitioner.

Although any device that contains a crypto image can be the registrar, it is recommended that the registrar be either a Cisco IOS certificate server registration authority (RA) or a Cisco IOS certificate server root.

Examples

The following sample output from the **show running-config** command verifies that the certificate server "cs1" was configured and associated with the TTI exchange between the registrar and petitioner:

```
crypto pki server cs1
 issuer-name CN = ioscs,L = Santa Cruz,C =US
 lifetime crl 336
 lifetime certificate 730
!
crypto pki trustpoint pki-36a
```

```
 enrollment url http://pki-36a:80
 ip-address FastEthernet0/0
 revocation-check none
!
crypto pki trustpoint cs1
 revocation-check crl
 rsakeypair cs1
!
!
crypto pki certificate chain pki-36a
 certificate 03
  308201D0 30820139 A0030201 02020103 300D0609 2A864886 F70D0101 04050030
  34310B30 09060355 04061302 55533114 30120603 55040713 0B205361 6E746120
  4372757A 310F300D 06035504 03130620 696F7363 73301E17 0D303430 31333130
  39333334 345A170D 30363031 33303039 33333434 5A303A31 38301606 092A8648
  86F70D01 09081309 31302E32 332E322E 32301E06 092A8648 86F70D01 09021611
  706B692D 3336612E 63697363 6F2E636F 6D305C30 0D06092A 864886F7 0D010101
  0500034B 00304802 4100AFFA 8F429618 112FAB9D 01F3352E 59DD3D2D AE67E31D
  370AC4DA 619735DF 9CF4EA13 64E4B563 C239C5F0 1578B773 07BED641 A18CA629
  191884B5 61B66ECF 4D110203 010001A3 30302E30 0B060355 1D0F0404 030205A0
  301F0603 551D2304 18301680 141DA8B1 71652961 3F7D69F0 02903AC3 2BADB137
  C6300D06 092A8648 86F70D01 01040500 03818100 67BAE186 327CED31 D642CB39
  AD585731 95868683 B950DF14 3BCB155A 2B63CFAD B34B579C 79128AD9 296922E9
  4DEDFCAF A7B5A412 AB1FC081 09951CE3 08BFFDD9 9FB1B9DA E9AA42C8 D1049268
  C524E58F 11C6BA7F C750320C 03DFB6D4 CBB3E739 C8C76359 CE939A97 B51B3F7F
  3FF;A9D82 9CFDB6CF E2503A14 36D0A236 A1CCFEAE
  quit
 certificate ca 01
  30820241 308201AA A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  34310B30 09060355 04061302 55533114 30120603 55040713 0B205361 6E746120
  4372757A 310F300D 06035504 03130620 696F7363 73301E17 0D303430 31333130
  39333132 315A170D 30373031 33303039 33313231 5A303431 0B300906 03550406
  13025553 31143012 06035504 07130B20 53616E74 61204372 757A310F 300D0603
  55040313 0620696F 73637330 819F300D 06092A86 4886F70D 01010105 0003818D
  00308189 02818100 FC0695AF 181CE90A 1B34B348 BA957178 680C8B51 07802AC3
  BF77B9C6 CB45092E 3C22292D C7D5FFC1 899185A1 FD8F37D5 C44FC206 6D1FA581
  E2264C83 1CC7453E 548C89C6 F3CD25BC 9BFFE7C5 E6653A06 62133950 78BED51B
  49128428 AB237F80 83A530EA 6F896193 F2134B54 D181F059 348AA84B 21EE6D80
  727BF668 EB004341 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
  01FF300E 0603551D 0F0101FF 04040302 0186301D 0603551D 0E041604 141DA8B1
  71652961 3F7D69F0 02903AC3 2BADB137 C6301F06 03551D23 04183016 80141DA8
  B1716529 613F7D69 F002903A C32BADB1 37C6300D 06092A86 4886F70D 01010405
  00038181 00885895 A0141169 3D754EB2 E6FEC293 5BF0A80B E424AA2F A3F59765
  3463AAD1 55E71F0F B5D1A35B 9EA79DAC DDB40721 1344C01E 015BAB73 1E148E03
  9DD01431 A5E2887B 4AEC8EF4 48ACDB66 A6F9401E 8F7CA588 8A4199BB F8A437A0
  F25064E7 112805D3 074A154F 650D09B9 8FA19347 ED359EAD 4181D9ED 0C667C10
  8A7BCFB0 FB
  quit
crypto pki certificate chain cs1
 certificate ca 01
  30820241 308201AA A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  34310B30 09060355 04061302 55533114 30120603 55040713 0B205361 6E746120
  4372757A 310F300D 06035504 03130620 696F7363 73301E17 0D303430 31333130
  39333132 315A170D 30373031 33303039 33313231 5A303431 0B300906 03550406
  13025553 31143012 06035504 07130B20 53616E74 61204372 757A310F 300D0603
  55040313 0620696F 73637330 819F300D 06092A86 4886F70D 01010105 0003818D
  00308189 02818100 FC0695AF 181CE90A 1B34B348 BA957178 680C8B51 07802AC3
  BF77B9C6 CB45092E 3C22292D C7D5FFC1 899185A1 FD8F37D5 C44FC206 6D1FA581
  E2264C83 1CC7453E 548C89C6 F3CD25BC 9BFFE7C5 E6653A06 62133950 78BED51B
  49128428 AB237F80 83A530EA 6F896193 F2134B54 D181F059 348AA84B 21EE6D80
  727BF668 EB004341 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
  01FF300E 0603551D 0F0101FF 04040302 0186301D 0603551D 0E041604 141DA8B1
  71652961 3F7D69F0 02903AC3 2BADB137 C6301F06 03551D23 04183016 80141DA8
  B1716529 613F7D69 F002903A C32BADB1 37C6300D 06092A86 4886F70D 01010405
```

```
  00038181 00885895 A0141169 3D754EB2 E6FEC293 5BF0A80B E424AA2F A3F59765
  3463AAD1 55E71F0F B5D1A35B 9EA79DAC DDB40721 1344C01E 015BAB73 1E148E03
  9DD01431 A5E2887B 4AEC8EF4 48ACDB66 A6F9401E 8F7CA588 8A4199BB F8A437A02;
  F25064E7 112805D3 074A154F 650D09B9 8FA19347 ED359EAD 4181D9ED 0C667C10
  8A7BCFB0 FB
  quit
!
crypto wui tti registrar
 pki-server cs1
!
!
!
crypto isakmp policy 1
 hash md5
!
!
crypto ipsec transform-set test_transformset esp-3des
!
crypto map test_cryptomap 10 ipsec-isakmp
 set peer 10.23.1.10
 set security-association lifetime seconds 1800
 set transform-set test_transformset
 match address 170
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.
crypto wui tti petitioner	Configures a device to become an EzSDD petitioner and enters tti-petitioner configuration mode.

crypto xauth

To configure crypto Extended Authentication (xauth) parameters globally on a per-interface basis, use the **crypto xauth** command in global configuration mode. To disable the xauth parameters, use the **no** form of this command.

crypto xauth *interface-name interface-number*

no crypto xauth *interface-name interface-number*

Syntax Description

interface-name	Name of the interface.
interface-number	Number of the related interface. Each interface has a related range of numbers. For example, the asynchronous interface has a range of interface numbers from 1 to 5 and the BVI interface has a range of interface numbers from 1 to 255.

Command Default

Crypto xauth parameters are not configured on any interface.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS 15.0(1)M.

Usage Guidelines

This command is mainly used on responders.

This command is used to disable the negotiation of xauth capabilities during proposals for a session that is terminating on a specific interface.

The **no crypto xauth** command enables the negotiation of xauth capabilities.

Examples

The following example shows how to enable crypto xauth parameters globally on a per-interface basis:

```
Router> enable
Router# configure terminal
Router(config)# crypto xauth fastethernet 0/1
```

The following example shows how the **no crypto xauth** command uses the nonvolatile generation (NVGEN) process to perform a configuration state retrieval operation when you specify the **show run** command:

```
Router> enable
Router# configure terminal
Router(config)# no crypto xauth fastethernet 0/1

Router# show run
archive
 log config
```

```
  hidekeys
!
redundancy
!
!
!
no crypto xauth Ethernet0/0
```

Related Commands

Command	Description
crypto key decrypt rsa	Deletes the encrypted RSA key and leaves only the unencrypted key on the running router.

csd enable

To enable Cisco Secure Desktop (CSD) support for SSL VPN sessions, use the **csd enable** command in webvpn context configuration mode. To remove CSD support from the SSL VPN context configuration, use the **no** form of this command.

csd enable

no csd enable

Syntax Description

This command has no keywords or arguments.

Command Default

CSD support is not enabled.

Command Modes

Webvpn context configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The CSD software installation package must be present in a local file system, such as flash memory, and it must be cached for distribution to end users (remote PC or networking device). The **webvpn install** command is used to install the software installation package to the distribution cache.

Examples

The following example enables CSD support for SSL VPN sessions:

```
Router(config)# webvpn install csd flash:/securedesktop_3_1_0_9.pkg
SSLVPN Package Cisco-Secure-Desktop : installed successfully
Router(config)# webvpn context context1
Router(config-webvpn-context)# csd enable
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.
webvpn install	Installs a CSD or SSL VPN client package file to a SSL VPN gateway for distribution to end users.

ctcp port

To set the port number for Cisco Tunneling Control Protocol (cTCP) encapsulation for Easy VPN, use the **ctcp port** command in crypto ipsec client ezvpn configuration mode. To disable the port that was configured, use the **no** form of this command.

ctcp port *port-number*

no ctcp port

Syntax Description

port-number	Port number. Value = 1 through 65535.

Command Default

If a port is not specified, the default port is the port on which the cTCP server listens.

Command Modes

Crypto ipsec client ezvpn configuration (config-crypto-ezvpn)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

This command is used only on the Easy VPN remote device.

Examples

The following example shows that the cTCP port number has been set to 10:

```
Router (config)# crypto ipsec client ezvpn client1
Router (config-crypto-ezvpn)# ctcp port 10
```

Related Commands

Command	Description
crypto ctcp	Configures cTCP encapsulation for Easy VPN.

ctype

To preauthenticate calls on the basis of the call type, use the **ctype** command in AAA preauthentication configuration mode. To remove the **ctype** command from your configuration, use the **no** form of this command.

ctype [**if-avail | required**] [**accept-stop**] [**password** *password*] [**digital | speech | v.110 | v.120**]

no ctype [**if-avail | required**] [**accept-stop**] [**password** *password*] [**digital | speech | v.110 | v.120**]

Syntax Description

if-avail	(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.
required	(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.
accept-stop	(Optional) Prevents subsequent preauthentication elements such as **clid** or **dnis** from being tried once preauthentication has succeeded for a call element.
password *password*	(Optional) Defines the password for the preauthentication element.
digital	(Optional) Specifies “digital” as the call type for preauthentication.
speech	(Optional) Specifies “speech” as the call type for preauthentication.
v.110	(Optional) Specifies “v.110” as the call type for preauthentication.
v.120	(Optional) Specifies “v.120” as the call type for preauthentication.

Defaults

The **if-avail** and **required** keywords are mutually exclusive. If the **if-avail** keyword is not configured, the preauthentication setting defaults to **required**.

The default password string is cisco.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You may configure more than one of the AAA preauthentication commands (**clid**, **ctype**, **dnis**) to set conditions for preauthentication. The sequence of the command configuration decides the sequence of the preauthentication conditions. For example, if you configure **dnis**, then **clid**, then **ctype**, in this order, then this is the order of the conditions considered in the preauthentication process.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

Set up the RADIUS preauthentication profile with the call type string as the username and with the password that is defined in the **ctype** command as the password. Table 28 shows the call types that you may use in the preauthentication profile.

Table 28 Preauthentication Call Types

Call Type String	ISDN Bearer Capabilities
digital	Unrestricted digital, restricted digital.
speech	Speech, 3.1 kHz audio, 7 kHz audio.
v.110	Anything with V.110 user information layer.
v.120	Anything with V.120 user information layer.

Examples

The following example specifies that incoming calls be preauthenticated on the basis of the call type:

```
aaa preauth
 group radius
 ctype required
```

Related Commands

Command	Description
clid	Preauthenticates calls on the basis of the CLID number.
dnis (RADIUS)	Preauthenticates calls on the basis of the DNIS number.
dnis bypass (AAA preauthentication configuration)	Specifies a group of DNIS numbers that will be bypassed for preauthentication.
group (RADIUS)	Specifies the AAA RADIUS server group to use for preauthentication.

data

To configure the data interface type and number for a redundancy group, use the **data** command in redundancy application group configuration mode**.** To remove the configuration, use the **no** form of this command.

data *interface-type interface-number*

no data *interface-type interface-number*

Syntax Description

interface-type	Interface type.
interface-number	Interface number.

Command Default

No data interface is configured.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

Use the **data** command to configure the data interface. The data interface can be the same physical interface as the control interface.

Examples

The following example shows how to configure the data Gigabit Ethernet interface for group1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# data GigabitEthernet 0/0/0
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
control	Configures the control interface type and number for a redundancy group.
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.

Command	Description
preempt	Enables preemption on the redundancy group.
protocol	Defines a protocol instance in a redundancy group.

database archive

To set the certification authority (CA) certificate and CA key archive format—and the password—to encrypt this CA certificate and CA key archive file, use the **database archive** command in certificate server configuration mode. To disable the autoarchive feature, use the **no** form of this command.

database archive {**pkcs12** | **pem**} [**password** *password*]

no database archive {**pkcs12** | **pem**} [**password** *password*]

Syntax Description

pkcs12	Export as a PKCS12 file. The default is PKCS12.
pem	Export as a privacy-enhanced mail (PEM) file.
password *password*	(Optional) Password to encrypt the CA certificate and CA key. The password must be at least eight characters. If a password is not specified, you will be prompted for the password after the **no shutdown** command has been issued for the first time. When the password is entered, it will be encrypted.

Defaults

The archive format is PKCS (that is, the CA certificate and CA key are exported into a PKCS12 file, and you will be prompted for the password when the certificate server is turned on the first time).

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

Use this command to configure the autoarchive format for the CA certificate and CA key. The archive can later be used to restore your certificate server.

If autoarchiving is not explicitly turned off when the certificate server is first enabled (using the **no shutdown** command), the CA certificate and CA key will be archived automatically, applying the following rule:

- The CA key must be (1) manually generated and marked “exportable” or (2) automatically generated by the certificate server (it will be marked nonexportable).

Note It is strongly recommended that if the password is included in the configuration to suppress the prompt after the **no shutdown** command, the password should be removed from the configuration after the archiving is finished.

Examples

The following example shows that certificate server autoarchiving has been enabled. The CA certificate and CA key format has been set to PEM, and the password has been set as cisco123.

```
Router (config)# crypto pki server myserver
Router (cs-server)# database archive pem password cisco123
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server.

database level

To control what type of data is stored in the certificate enrollment database, use the **database level** command in certificate server configuration mode. To return to the default functionality, use the **no** form of this command.

database level {**minimal** | **names** | **complete**}

no database level {**minimal** | **names** | **complete**}

Syntax Description

minimal	Enough information is stored only to continue issuing new certificates without conflict. This is the default functionality.
names	The serial number and subject name of each certificate are stored in the database, providing enough information for the administrator to find and revoke and particular certificate, if necessary.
complete	Each issued certificate is written to the database. If this keyword is used, you should enable the **database url** command; see "Usage Guidelines" for more information.

Defaults

minimal

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The **database level** command is used to describe the database of certificates and certification authority (CA) states. After the user downgrades the database level, the old data stays the same and the new data is logged at the new level.

minimum Level

The *ca-label*.ser file is always available. It contains the previously issued certificate's serial number, which is always 1. If the .ser file is unavailable and the CA server has a self-signed certificate in the local configuration, the CA server will refuse to issue new certificates.

The file format is as follows:

```
last_serial = serial-number
```

names Level

The *serial-number*.cnm file, which is written for each issued certificate, contains the "human readable decoded subject name" of the issued certificate and the "der encoded" values. This file can also include a certificate expiration date and the current status. (The **minimum** level files are also written out.)

The file format is as follows:

```
subjectname_der = <base64 encoded der value>
subjectname_str = <human readable decode subjectname>
expiration = <expiration date>
status = valid | revoked
```

complete Level

The *serial-number*.cer file, which is written for each issued certificate, is the binary certificate without additional encoding. (The **minimum** and **names** level files are also written out.)

The **complete** level produces a large amount of information, so you may want to store all database entries on an external TFTP server via the **database url** command unless your router does one of the following:

- Issues only a small number of certificates
- Has a local file system that is designed to support a large number of write operations and has sufficient storage for the certificates that are being issued

Examples

The following example shows how configure a minimum database to be stored on the local system:

```
Router#(config) ip http server
Router#(config) crypto pki server myserver
Router#(cs-server) database level minimum
Router#(cs-server) database url nvram:
Router#(cs-server) issuer-name CN = ipsec_cs,L = Santa Cruz,C = US
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters PKI configuration mode.
database url	Specifies the location where all database entries for the certificate server will be written out.

database url

To specify the location where database entries for the certificate server (CS) will be stored or published, use the **database url** command in certificate server configuration mode. To return to the default location, use the **no** form of this command.

Storing Files to a Primary Location

database url *root-url*

Storing Critical CS Files to a Specific Location

database url [{**cnm** | **crl** | **crt** | **p12** | **pem** | **ser**}] *root-url* [**username** *username*] [**password** [*encrypt-type*] *password*]

no database url [{**cnm** | **crl** | **crt** | **p12** | **pem** | **ser**}] *root-url* [**username** *username*] [**password** [*encrypt-type*] *password*]

Publishing Noncritical CS Files to a Specific Location

database url {**cnm** | **crl** | **crt**} **publish** *root-url* [**username** *username*][**password** [*encrypt-type*] *password*]

no database url {**cnm** | **crl** | **crt**} **publish** *root-url* [**username** *username*][**password** [*encrypt-type*] *password*]

Syntax Description

root-url	Location where database entries will be written out. The URL can be any URL that is supported by the Cisco IOS file system (IFS).
cnm	(Optional) Specifies the certificate name and expiration file to be stored or published to a specific location.
crl	(Optional) Specifies the DER-encoded certificate revocation list to be stored or published to a specific location
crt	(Optional) Specifies the DER-encoded certificate files to be stored or published to a specific location.
p12	(Optional) Specifies the CS certificate and key archive file in PKCS12 format to be stored to a specific location.
pem	(Optional) Specifies the CS certificate and key archive file in privacy-enhanced mail format to be stored to a specific location.
ser	(Optional) Specifies the current serial number to be stored to a specific location.
publish	Specifies that the files will be made available to a published location.
username *username*	(Optional) When prompted, a username will be used to access a storage location.

password *password*	(Optional) When prompted, a password will be used to access a storage location.
encrypt-type	(Optional) Type of encryption to be used for the password. If no password type is specified the password is sent as clear text. • Default is 0; specifies that the password entered will be encrypted. • 7; specifies that the password entered is already encrypted.

Defaults

The default file storage location is flash.

No default file publish location is specified.

Command Modes

Certificate server configuration (cs-server)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(4)T	This command was modified. The following keywords and arguments were added **cnm**, **crl**, **crt**, **p12**, **pem**, **ser**, **publish, username** *username***,** *encrypt-type* and **password** *password*.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.

Usage Guidelines

After you create a certificate server via the **crypto pki server** command, use the **database url** command if you want to specify a combined list of all the certificates that have been issued and the current command revocation list (CRL). The CRL is written to the certificate enrollment database as *ca-label*.crl (where *ca-label* is the name of the certificate server).

Note Although issuing the **database url** command is not required, it is recommended. Unless your router has a local file system that is designed for a large number of write operations and has sufficient storage for the certificates that are issued, you should issue this command.

Cisco IOS File System

The router uses any file system that is supported by your version of Cisco IOS software (such as TFTP, FTP, flash, and NVRAM) to send a certificate request and to receive the issued certificate. A user may wish to enable IFS certificate enrollment when his or her certification authority (CA) does not support Simple Certificate Enrollment Protocol (SCEP).

Specifying CS Storage and Publication Location by File Type

The CS allows the flexibility to store different critical file types to specific storage locations and publish non-critical files to the same or alternate locations. When choosing storage locations consider the file security needed and server performance. For instance, serial number files (.ser) and archive files (.p12 or .pem) might have greater security restrictions than the general certificates storage location (.crt) or the name file storage location (.cnm). Performance of your certificate server may be affected by the storage location(s) you choose, for example, reading from a network location would likely take more time than reading directly from a router's local storage device.

Examples

The following example shows how to configure all database entries to be written out to a TFTP server:

```
Router#(config) ip http server
Router#(config) crypto pki server myserver
Router#(cs-server) database level complete
Router#(cs-server) database url tftp://mytftp
```

The following example shows the configuration of a primary storage location for critical files, a specific storage location for the critical file serial number file, the main CS database file, and a password protected file publication location for the CRL file:

```
Router(config)# crypto pki server mycs
Router(cs-server)# database url ftp://cs-db.company.com
!
% Server database url was changed. You need to move the
% existing database to the new location.
!
Router(cs-server)# database url ser nvram:
Router(cs-server)# database url crl publish ftp://crl.company.com username myname password
mypassword
Router(cs-server)# end
```

The following show output displays the specified primary storage location and critical file storage locations specified:

```
Router# show

Sep  3 20:19:34.216: %SYS-5-CONFIG_I: Configured from console by user on console
Router# show crypto pki server

Certificate Server mycs:
     Status: disabled
     Server's configuration is unlocked  (enter "no shut" to lock it)
     Issuer name: CN=mycs
     CA cert fingerprint: -Not found-
     Granting mode is: manual
     Last certificate issued serial number: 0x0
     CA certificate expiration timer: 00:00:00 GMT Jan 1 1970
     CRL not present.
     Current primary storage dir: ftp://cs-db.company.com
     Current storage dir for .ser files: nvram:
     Database Level: Minimum - no cert data written to storage
Router#
```

The following show output displays all storage and publication locations. The serial number file (.ser) is stored in NVRAM. The CRL file will be published to ftp://crl.company.com with a username and password. All other critical files will be stored to the primary location, ftp://cs-db.company.com.

```
Router# show running-config

   section crypto pki server
   crypto pki server mycs shutdown database url ftp://cs-db.company.com
   database url crl publish ftp://crl.company.com username myname password 7
12141C0713181F13253920
   database url ser nvram:
Router#
```

Verifying the Database URL

To ensure that the specified URL is working correctly, configure the **database url** command before you issue the **no shutdown** command on the certificate server for the first time. If the URL is broken, you will see output as follows:

```
Router(config)# crypto pki server mycs
Router(cs-server)# database url ftp://myftpserver
Router(cs-server)# no shutdown
% Once you start the server, you can no longer change some of
% the configuration.
Are you sure you want to do this? [yes/no]: yes
Translating "myftpserver"
% There was a problem reading the file 'mycs.ser' from certificate storage.
% Please verify storage accessibility and enable the server again.

% Failed to generate CA certificate - 0xFFFFFFFF
% The Certificate Server has been disabled.
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters PKI server configuration mode.
database level	Controls what type of data is stored in the database.
database username	Requires a username or password to be issued when accessing the primary database storage location.

database username

To require a username or password to be issued when accessing the primary database location, use the **database username** command in certificate server configuration mode. To return to the default value, use the **no** form of this command.

database username *username* [**password** [*encr-type*] *password*]

no database username *username* [**password** [*encr-type*] *password*]

Syntax Description

username	When prompted, a username will be used to access a storage location.
password *password*	(Optional) When prompted, a password will be used to access a storage location.
encr-type	(Optional) Type of encryption to be used for the password. If no password encryption type is specified, the password is sent as clear text. • Default is 0; specifies that the password entered will be encrypted. • 7; specifies the password entered is already encrypted.

Defaults

No username or password will be used to access the primary database storage location.

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(4)T	The command name was changed from **database** (certificate server) to **database username**.

Usage Guidelines

All information stored in the remote database is public: there are no private keys stored in the database location. Using a password helps to protect against a potential attacker who can change the contents of the .ser or .crl file. If the contents of the files are changed, the certificate server may shut down, refusing to either issue new certificates or respond to Simple Certificate Enrollment Protocol (SCEP) requests until the files are restored.

It is good security practice to protect all information exchanges with the database server using IP Security (IPsec). To protect your information, use a remote database to obtain the appropriate certificates and setup the necessary IPsec connections to protect all future access to the database server.

Examples

The following example shows how to specify the username “mystorage” when the primary storage location is on an external TFTP server:

```
Router (config)# ip http server
Router (config)# crypto pki server myserver
Router (cs-server)# database level complete
```

```
Router (cs-server)# database url tftp://mytftp
Router (cs-server)# database username mystorage
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters PKI server configuration mode.
database level	Controls what type of data is stored in the database.
database url	Specifies the primary storage location for the certificate server.

deadtime (server-group configuration)

To configure deadtime within the context of RADIUS server groups, use the **deadtime** command in server group configuration mode. To set deadtime to 0, use the **no** form of this command.

deadtime *minutes*

no deadtime

Syntax Description

minutes	Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests, up to a maximum of 1440 minutes (24 hours).

Defaults

Deadtime is set to 0.

Command Modes

Server-group configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to configure the deadtime value of any RADIUS server group. The value of deadtime set in the server groups will override the server that is configured globally. If deadtime is omitted from the server group configuration, the value will be inherited from the master list. If the server group is not configured, the default value (0) will apply to all servers in the group.

When the RADIUS Server Is Marked As Dead

For Cisco IOS versions prior to 12.2(13.7)T, the RADIUS server will be marked as dead if a transaction is transmitted for the configured number of retransmits and a valid response is not received from the server within the configured timeout for any of the RADIUS packet transmissions.

For Cisco IOS versions 12.2(13.7)T and later, the RADIUS server will be marked as dead if both of the following conditions are met:

1. A valid response has not been received from the RADIUS server for any outstanding transaction for at least the timeout period that is used to determine whether to retransmit to that server, and
2. Across all transactions being sent to the RADIUS server, at least the requisite number of retransmits +1 (for the initial transmission) have been sent consecutively without receiving a valid response from the server with the requisite timeout.

Examples

The following example specifies a one-minute deadtime for RADIUS server group group1 once it has failed to respond to authentication requests:

```
aaa group server radius group1
 server 10.1.1.1 auth-port 1645 acct-port 1646
 server 10.2.2.2 auth-port 2000 acct-port 2001
 deadtime 1
```

Related Commands

Command	Description
radius-server deadtime	Sets the deadtime value globally.

default (ca-trustpoint)

To reset the value of a ca-trustpoint configuration subcommand to its default, use the **default** command in ca-trustpoint configuration mode.

default *command-name*

Syntax Description

command-name	Ca-trustpoint configuration subcommand.

Defaults

No default behavior or values.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(8)T	The command mode was changed from **default (ca-root)** to **default (ca-trustpoint)** to support the **crypto ca trustpoint** command and all related subcommands.
12.2(18)SXD	The **default (ca-root)** command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	The **default (ca-root)** command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Before you can configure this command, you must enable the **crypto ca trustpoint** command, which enters ca-trustpoint configuration mode.

Use this command to reset the value of a ca-trustpoint configuration mode subcommand to its default.

Note The **crypto ca trustpoint** command deprecates the **crypto ca identity** and **crypto ca trusted-root** commands and all related subcommands (all ca-identity and trusted-root configuration mode commands). If you enter a ca-identity or trusted-root subcommand, the configuration mode and command will be written back as ca-trustpoint.

Examples

The following example shows how to remove the **crl optional** command from your configuration; the default of **crl optional** is off.

```
default crl optional
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

default-group-policy

To associate a policy group with a SSL VPN context configuration, use the **default-group-policy** command in webvpn context configuration mode. To remove the policy group from the webvpn context configuration, use the **no** form of this command.

default-group-policy *name*

no default-group-policy

Syntax Description

name	Name of the policy configured with the **policy group** command.

Command Default

A policy group is not associated with a SSL VPN context configuration.

Command Modes

Webvpn context configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The **policy group** command is first configured to define policy group configuration parameters. This command is configured to attach the policy group to the SSL VPN context when multiple policy groups are defined under the context. This policy will be used as the default unless an authentication, authorization, and accounting (AAA) server pushes an attribute that specifically requests another group policy.

Examples

The following example configures policy group ONE as the default policy group:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy-group ONE
Router(config-webvpn-group)# exit
Router(config-webvpn-context)# policy-group TWO
Router(config-webvpn-group)# exit
Router(config-webvpn-context)# default-group-policy ONE
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

deny

To set conditions in a named IP access list or object group access control list (OGACL) that will deny packets, use the **deny** configuration command in the appropriate configuration mode. To remove a deny condition from an IP access list or OGACL, use the **no** form of this command.

deny *protocol* {{*source-addr source-wildcard*} | **object-group** *object-group-name* | **any** | **host** {*address* | *name*}} {*destination-addr destination-wildcard*} | **object-group** *object-group-name* | **any** | **host** {*address* | *name*}}

deny {**tcp** | **udp**} {{*source-addr source-wildcard*} | **object-group** *source-addr-group-name* | **any** | **host** {*address* | *name*} {*destination-addr destination-wildcard* | **any** | **eq** *port* | **gt** *port* | **host** {*address* | *name*} | **lt** *port* | **neq** *port* | **portgroup** *srcport-groupname*} {**object-group** *dest-addr-groupname* | *destination* | *destination-addr destination-wildcard* | **any** | **eq** *port* | **gt** *port* | **host** {*address* | *name*} | **lt** *port* | **neq** *port* | **portgroup** *destport-groupname*} [**dscp** *type*] [**fragments**] [**option** *option*] [**precedence** *precedence*] [**log**] [**log-input**] [**time-range** *time-range-name*] [**tos** *tos*]]}

no deny *protocol* {{*source-addr source-wildcard*} | **object-group** *object-group-name* | **any** | **host** {*address* | *name*}} {*destination-addr destination-wildcard*} | **object-group** *object-group-name* | **any** | **host** {*address* | *name*}}

no deny {**tcp** | **udp**} {{*source-addr source-wildcard*} | **object-group** *source-addr-group-name* | **any** | **host** {*address* | *name*} {*destination-addr destination-wildcard* | **any** | **eq** *port* | **gt** *port* | **host** {*address* | *name*} | **lt** *port* | **neq** *port* | **portgroup** *srcport-groupname*} {**object-group** *dest-addr-groupname* | *destination* | *destination-addr destination-wildcard* | **any** | **eq** *port* | **gt** *port* | **host** {*address* | *name*} | **lt** *port* | **neq** *port* | **portgroup** *destport-groupname*} [**dscp** *type*] [**fragments**] [**option** *option*] [**precedence** *precedence*] [**log**] [**log-input**] [**time-range** *time-range-name*] [**tos** *tos*]]}

Syntax Description

protocol	Name or number of a protocol; valid values are **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, or **udp**, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP), use the keyword **ip**. See the "Usage Guidelines" section for additional qualifiers.
source-addr	Number of the network or host from which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.
source-wildcard	Wildcard bits to be applied to source in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.
object-group *object-group-name*	Specifies the source or destination name of the object group.
any	Specifies any source or any destination host as an abbreviation for the *source-addr* or *destination-addr* value and the *source-wildcard* or *destination-wildcard* value of 0.0.0.0 255.255.255.255.
host *address*	Specifies the source or destination address of a single host.
host *name*	Specifies the source or destination name of a single host.
tcp	Specifies the TCP protocol.
udp	Specifies the UDP protocol.

object-group *source-addr-group-name*	Specifies the source address group name.
destination-addr	Number of the network or host to which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.
destination-wildcard	Wildcard bits to be applied to the destination in a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.
eq *port*	Matches only packets on a given port number; see the "Usage Guidelines" section for valid values.
gt *port*	Matches only the packets with a greater port number; see the "Usage Guidelines" section for valid values.
lt *port*	Matches only the packets with a lower port number; see the "Usage Guidelines" section for valid values.
neq *port*	Matches only the packets that are not on a given port number; see the "Usage Guidelines" section for valid values.
portgroup *srcport-group-name*	Specifies the source port object group name.
object-group *dest-addr-group-name*	Specifies the destination address group name.
portgroup *destport-group-name*	Specifies the destination port object group name.
dscp *type*	(Optional) Matches the packets with the given Differentiated Services Code Point (DSCP) value; see the "Usage Guidelines" section for valid values.
fragments	(Optional) Applies the access list entry to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the "Access List Processing of Fragments" and "Fragments and Policy Routing" sections in the "Usage Guidelines" section.
option *option*	(Optional) Matches the packets with the given IP options value number; see the "Usage Guidelines" section for valid values.
precedence *precedence*	(Optional) Specifies the precedence filtering level for packets; valid values are a number from 0 to 7 or by a name. See the "Usage Guidelines" section for a list of valid names.

object-group *source-addr-group-name*	Specifies the source address group name.
destination-addr	Number of the network or host to which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.
destination-wildcard	Wildcard bits to be applied to the destination in a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.
eq *port*	Matches only packets on a given port number; see the "Usage Guidelines" section for valid values.
gt *port*	Matches only the packets with a greater port number; see the "Usage Guidelines" section for valid values.
lt *port*	Matches only the packets with a lower port number; see the "Usage Guidelines" section for valid values.
neq *port*	Matches only the packets that are not on a given port number; see the "Usage Guidelines" section for valid values.
portgroup *srcport-group-name*	Specifies the source port object group name.
object-group *dest-addr-group-name*	Specifies the destination address group name.
portgroup *destport-group-name*	Specifies the destination port object group name.
dscp *type*	(Optional) Matches the packets with the given Differentiated Services Code Point (DSCP) value; see the "Usage Guidelines" section for valid values.
fragments	(Optional) Applies the access list entry to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the "Access List Processing of Fragments" and "Fragments and Policy Routing" sections in the "Usage Guidelines" section.
option *option*	(Optional) Matches the packets with the given IP options value number; see the "Usage Guidelines" section for valid values.
precedence *precedence*	(Optional) Specifies the precedence filtering level for packets; valid values are a number from 0 to 7 or by a name. See the "Usage Guidelines" section for a list of valid names.

log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message for a standard list includes the access list number, whether the packet was permitted or denied, the source address, and the number of packets. The message for an extended list includes the access list number; whether the packet was permitted or denied; the protocol; whether the protocol was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. For both standard and extended lists, the message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from reloading because of too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.
log-input	(Optional) Matches the log against this entry, including the input interface.
time-range *time-range-name*	(Optional) Specifies a time-range entry name.
tos *tos*	(Optional) Specifies the service filtering level for packets; valid values are a number from 0 to 15 or by a name as listed in the "Usage Guidelines" section of the **access-list** (IP extended) command.
option *option*	(Optional) Matches packets with the IP options value; see the "Usage Guidelines" section for the valid values.
fragments	(Optional) Applies the access list entry to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the "Access List or OGACL Processing of Fragments" and "Fragments and Policy Routing" sections in the "Usage Guidelines" section.

Command Default

There is no specific condition under which a packet is denied passing the access list.

Command Modes

Standard access-list configuration (config-std-nacl)
Extended access-list configuration (config-ext-nacl)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Use this command following the **ip access-list** command to specify conditions under which a packet cannot pass the access list.

The **portgroup** keyword appears only when you configure an extended ACL.

The *address* or *object-group-name* value is created using the **object-group** command.

The **object-group** *object-group-name* keyword and argument allow you to create logical groups of users (or servers), which you can use to define access policy using ACLs. For example, with one ACL entry you can permit the object group named engineering to access all engineering servers. Otherwise, you would need one ACL entry for every person in the engineering group.

If the operator is positioned after the *source-addr* and *source-wildcard* values, it must match the source port.

If the operator is positioned after the *destination-addr* and *destination-wildcard* values, it must match the destination port.

If you are entering the port number of a TCP or UDP port, you can enter the decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the "Usage Guidelines" section of the **access-list** (IP extended) command. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.

The valid values for the **dscp** *type* keyword and argument are as follows:

- **0** to **63**—Differentiated services code point value.
- **af11**—Match packets with AF11 dscp (001010).
- **af12**—Match packets with AF12 dscp (001100).
- **af13**—Match packets with AF13 dscp (001110).
- **af21**—Match packets with AF21 dscp (010010).
- **af22**—Match packets with AF22 dscp (010100).
- **af23**—Matches the patches with the AF23 dscp (010110).
- **af31**—Matches the patches with the AF31 dscp (011010).
- **af32**—Matches the patches with the AF32 dscp (011100).
- **af33**—Matches the patches with the AF33 dscp (011110).
- **af41**—Matches the patches with the AF41 dscp (100010).
- **af42**—Matches the patches with the AF42 dscp (100100).
- **af43**—Matches the patches with the AF43 dscp (100110).
- **cs1**—Matches the patches with the CS1 (precedence 1) dscp (001000).
- **cs2**—Matches the patches with the CS2 (precedence 2) dscp (010000).
- **cs3**—Matches the patches with the CS3 (precedence 3) dscp (011000).
- **cs4**—Matches the patches with the CS4 (precedence 4) dscp (100000).
- **cs5**—Matches the patches with the CS5 (precedence 5) dscp (101000).
- **cs6**—Matches the patches with the CS6 (precedence 6) dscp (110000).
- **cs7**—Matches the patches with the CS7 (precedence 7) dscp (111000).
- **default**—Matches the patches with the default dscp (000000).
- **ef**—Matches the patches with the EF dscp (101110).

The valid values for the **eq** *port* keyword and argument are as follows:

- **0** to **65535**—Port number.
- **bgp**—Border Gateway Protocol (179).
- **chargen**—Character generator (19).
- **cmd**—Remote commands (rcmd, 514).
- **daytime**—Daytime (13).
- **discard**—Discard (9).
- **domain**—Domain Name Service (53).
- **echo**—Echo (7).
- **exec**—Exec (rsh, 512).
- **finger**—Finger (79).
- **ftp**—File Transfer Protocol (21).
- **ftp-data**—FTP data connections (20).
- **gopher**—Gopher (70).
- **hostname**—NIC hostname server (101).
- **ident**—Ident Protocol (113).
- **irc**—Internet Relay Chat (194).
- **klogin**—Kerberos login (543).
- **kshell**—Kerberos shell (544).
- **login**—Login (rlogin, 513).
- **lpd**—Printer service (515).
- **nntp**—Network News Transport Protocol (119).
- **pim-auto-rp**—PIM Auto-RP (496).
- **pop2**—Post Office Protocol v2 (109).
- **pop3**—Post Office Protocol v3 (110).
- **smtp**—Simple Mail Transport Protocol (25).
- **sunrpc**—Sun Remote Procedure Call (111).
- **syslog**—Syslog (514).
- **tacacs**—TAC Access Control System (49).
- **talk**—Talk (517).
- **telnet**—Telnet (23).
- **time**—Time (37).
- **uucp**—Unix-to-Unix Copy Program (540).
- **whois**—Nicname (43).
- **www**—World Wide Web (HTTP, 80).

The valid values for the **gt** *port* keyword and argument are as follows:

- **0**-**65535**—Port number.
- **biff**—Biff (mail notification, comsat, 512).
- **bootpc**—Bootstrap Protocol (BOOTP) client (68).

- **bootps**—Bootstrap Protocol (BOOTP) server (67).
- **discard**—Discard (9).
- **dnsix**—DNSIX security protocol auditing (195).
- **domain**—Domain Name Service (DNS, 53).
- **echo**—Echo (7).
- **isakmp**—Internet Security Association and Key Management Protocol (500).
- **mobile-ip**—Mobile IP registration (434).
- **nameserver**—IEN116 name service (obsolete, 42).
- **netbios-dgm**—NetBios datagram service (138).
- **netbios-ns**—NetBios name service (137).
- **netbios-ss**—NetBios session service (139).
- **non500-isakmp**—Internet Security Association and Key Management Protocol (4500).
- **ntp**—Network Time Protocol (123).
- **pim-auto-rp**—PIM Auto-RP (496).
- **rip**—Routing Information Protocol (router, in.routed, 520).
- **snmp**—Simple Network Management Protocol (161).
- **snmptrap**—SNMP Traps (162).
- **sunrpc**—Sun Remote Procedure Call (111).
- **syslog**—System Logger (514).
- **tacacs**—TAC Access Control System (49).
- **talk**—Talk (517).
- **tftp**—Trivial File Transfer Protocol (69).
- **time**—Time (37).
- **who**—Who service (rwho, 513).
- **xdmcp**—X Display Manager Control Protocol (177).

The valid values for the **lt** *port* keyword and argument are as follows:

- **0-65535**—Port number.
- **biff**—Biff (mail notification, comsat, 512).
- **bootpc**—Bootstrap Protocol (BOOTP) client (68).
- **bootps**—Bootstrap Protocol (BOOTP) server (67).
- **discard**—Discard (9).
- **dnsix**—DNSIX security protocol auditing (195).
- **domain**—Domain Name Service (DNS, 53).
- **echo**—Echo (7).
- **isakmp**—Internet Security Association and Key Management Protocol (500).
- **mobile-ip**—Mobile IP registration (434).
- **nameserver**—IEN116 name service (obsolete, 42).
- **netbios-dgm**—NetBios datagram service (138).

- **netbios-ns**—NetBios name service (137).
- **netbios-ss**—NetBios session service (139).
- **non500-isakmp**—Internet Security Association and Key Management Protocol (4500).
- **ntp**—Network Time Protocol (123).
- **pim-auto-rp**—PIM Auto-RP (496).
- **rip**—Routing Information Protocol (router, in.routed, 520).
- **snmp**—Simple Network Management Protocol (161).
- **snmptrap**—SNMP Traps (162).
- **sunrpc**—Sun Remote Procedure Call (111).
- **syslog**—System Logger (514).
- **tacacs**—TAC Access Control System (49).
- **talk**—Talk (517).
- **tftp**—Trivial File Transfer Protocol (69).
- **time**—Time (37).
- **who**—Who service (rwho, 513).
- **xdmcp**—X Display Manager Control Protocol (177).

The valid values for the **neg** *port* keyword and argument are as follows:

- **0** to **65535**—Port number.
- **biff**—Biff (mail notification, comsat, 512).
- **bootpc**—Bootstrap Protocol (BOOTP) client (68).
- **bootps**—Bootstrap Protocol (BOOTP) server (67).
- **discard**—Discard (9).
- **dnsix**—DNSIX security protocol auditing (195).
- **domain**—Domain Name Service (DNS, 53).
- **echo**—Echo (7).
- **isakmp**—Internet Security Association and Key Management Protocol (500).
- **mobile-ip**—Mobile IP registration (434).
- **nameserver**—IEN116 name service (obsolete, 42).
- **netbios-dgm**—NetBios datagram service (138).
- **netbios-ns**—NetBios name service (137).
- **netbios-ss**—NetBios session service (139).
- **non500-isakmp**—Internet Security Association and Key Management Protocol (4500).
- **ntp**—Network Time Protocol (123).
- **pim-auto-rp**—PIM Auto-RP (496).
- **rip**—Routing Information Protocol (router, in.routed, 520).
- **snmp**—Simple Network Management Protocol (161).
- **snmptrap**—SNMP Traps (162).
- **sunrpc**—Sun Remote Procedure Call (111).

- **syslog**—System Logger (514).
- **tacacs**—TAC Access Control System (49).
- **talk**—Talk (517).
- **tftp**—Trivial File Transfer Protocol (69).
- **time**—Time (37).
- **who**—Who service (rwho, 513).
- **xdmcp**—X Display Manager Control Protocol (177).

The valid values for the **option** *option* keyword and argument are as follows:

- **0** to **255**—IP Options value.
- **add-ext**—Matches the packets with Address Extension Option (147).
- **any-options**—Matches the packets with ANY Option.
- **com-security**—Matches the packets with Commercial Security Option (134).
- **dps**—Matches the packets with Dynamic Packet State Option (151).
- **encode**—Matches the packets with Encode Option (15).
- **eool**—Matches the packets with End of Options (0).
- **ext-ip**—Matches the packets with the Extended IP Option (145).
- **ext-security**—Matches the packets with the Extended Security Option (133).
- **finn**—Matches the packets with the Experimental Flow Control Option (205).
  - **imitd**—Matches the packets with IMI Traffic Desriptor Option (144).
  - **lsr**—Matches the packets with Loose Source Route Option (131).
  - **match-all**—Matches the packets if all specified flags are present.
  - **match-any**—Matches the packets if any specified flag is present.
  - **mtup**—Matches the packets with MTU Probe Option (11).
  - **mtur**—Matches the packets with MTU Reply Option (12).
  - **no-op**—Matches the packets with No Operation Option (1).
  - **psh**—Match the packets on the PSH bit.
  - **nsapa**—Matches the packets with NSAP Addresses Option (150).
  - **reflect**—Creates reflexive access list entry.
  - **record-route**—Matches the packets with Record Route Option (7).
  - **rst**—Matches the packets on the RST bit.
  - **router-alert**—Matches the packets with Router Alert Option (148).
  - **sdb**—Matches the packets with Selective Directed Broadcast Option (149).
  - **security**—Matches the packets with Basic Security Option (130).
  - **ssr**—Matches the packets with Strict Source Routing Option (137).
  - **stream-id**—Matches the packets with Stream ID Option (136).
  - **syn**—Match the packets on the SYN bit.
- **timestamp**—Matches the packets with the Time Stamp Option (68).
- **traceroute**—Matches the packets with the Trace Route Option (82).

- **ump**—Matches the packets with the Upstream Multicast Packet Option (152).
- **visa**—Matches the packets with the Experimental Access Control Option (142).
- **zsu**—Matches the packets with the Experimental Measurement Option (10).

The valid values for the **tos** *value* keyword and argument are as follows:

- **0** to **15**—Type of service value.
- **max-reliability**—Matches the packets with the maximum reliable ToS (2).
- **max-throughput**—Matches the packets with the maximum throughput ToS (4).
- **min-delay**—Matches the packets with the minimum delay ToS (8).
- **min-monetary-cost**—Matches packets with the minimum monetary cost ToS (1).
- **normal**—Matches the packets with the normal ToS (0).

Access List or OGACL Processing of Fragments

The behavior of access-list entries regarding the use or lack of the **fragments** keyword are summarized in Table 29:

Table 29 Access list or OGACL Processing of Fragments

If the Access-List Entry Has...	Then...
...no **fragments** keyword (the default behavior), and assuming all of the access-list entry information matches,	For an access-list entry containing only Layer 3 information: • The entry is applied to nonfragmented packets, initial fragments, and noninitial fragments. For an access list entry containing Layer 3 and Layer 4 information: • The entry is applied to nonfragmented packets and initial fragments: – If the entry is a **permit** statement, the packet or fragment is permitted. – If the entry is a **deny** statement, the packet or fragment is denied. • The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access-list entry can be applied. If the Layer 3 portion of the access-list entry matches, and – If the entry is a **permit** statement, the noninitial fragment is permitted. – If the entry is a **deny** statement, the next access-list entry is processed. **Note** The **deny** statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.
...the **fragments** keyword, and assuming all of the access-list entry information matches,	**Note** The access-list entry is applied only to noninitial fragments. The **fragments** keyword cannot be configured for an access-list entry that contains any Layer 4 information.

Be aware that you should not simply add the **fragments** keyword to every access list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments** keyword, the packet is compared to the next access list entry, and so on, until it is either permitted or denied by an access list entry that does not contain the **fragments** keyword. Therefore, you may need two access list entries for every **deny** entry. The first **deny** entry of the pair will not include the **fragments** keyword, and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases where there are multiple **deny** access-list entries for the same host but with different Layer 4 ports, a single **deny** access-list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets and each counts individually as a packet in access list accounting and access list violation counts.

Note The **fragments** keyword cannot solve all cases involving access lists and IP fragments.

Fragments and Policy Routing

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip address**s command and the access list had entries that match on Layer 4 through 7 information. It is possible that noninitial fragments pass the access list and are policy routed, even if the first fragment was not policy routed or the reverse.

By using the **fragments** keyword in access list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made and it is more likely policy routing will occur as intended.

The **portgroup** *srcport-groupname or* **portgroup** *destport-groupname* keywords and arguments allow you to create an object group based on a source or destination group.

Examples

The following example creates an access list that denies all TCP packets:

```
Router> enable
Router# configure terminal
Router(config)# ip access-list extended my_ogacl_policy
Router(config-ext-nacl)# deny tcp any any
Router(config-ext-nacl)# exit
Router(config)# exit
```

Related Commands

Command	Description
ip access-group	Applies an ACL or OGACL to an interface or a service policy map.
ip access-list	Defines an IP access list or OGACL by name or number.
object-group network	Defines network object groups for use in OGACLs.
object-group service	Defines service object groups for use in OGACLs.
permit	Sets conditions in a named IP access list or OGACL that will permit packets.
show ip access-list	Displays the contents of IP access lists or OGACLs.
show object-group	Displays information about object groups that are configured.

deny (Catalyst 6500 series switches)

To set conditions for a named access list, use the **deny** configuration command in access-list configuration mode. To remove a deny condition from an access list, use the **no** form of this command.

deny *protocol* {{*source-addr source-wildcard*} | **addrgroup** *object-group-name* | **any** | **host** {*address* | *name*}} {*destination-addr destination-wildcard*} | **addrgroup** *object-group-name* | **any** | **host** {*address* | *name*}}

deny {**tcp** | **udp**} {{*source-addr source-wildcard*} | **addrgroup** *source-addr-group-name* | **any** | **host** {*address* | *name*} {*destination-addr destination-wildcard* | **any** | **eq** *port* | **gt** *port* | **host** {*address* | *name*} | **lt** *port* | **neq** *port* | **portgroup** *srcport-groupname*} {**addrgroup** *dest-addr-groupname* | *destination* | *destination-addr destination-wildcard* | **any** | **eq** *port* | **gt** *port* | **host** {*address* | *name*} | **lt** *port* | **neq** *port* | **portgroup** *destport-groupname*} [**dscp** *type*] [**fragments**] [**option** *option*] [**precedence** *precedence*] [**log**] [**log-input**] [**time-range** *time-range-name*] [**tos** *tos*]]}

no deny *protocol* {{*source-addr source-wildcard*} | **addrgroup** *object-group-name* | **any** | **host** {*address* | *name*}} {*destination-addr destination-wildcard*} | **addrgroup** *object-group-name* | **any** | **host** {*address* | *name*}}

no deny {**tcp** | **udp**} {{*source-addr source-wildcard*} | **addrgroup** *source-addr-group-name* | **any** | **host** {*address* | *name*} {*destination-addr destination-wildcard* | **any** | **eq** *port* | **gt** *port* | **host** {*address* | *name*} | **lt** *port* | **neq** *port* | **portgroup** *srcport-groupname*} {**addrgroup** *dest-addr-groupname* | *destination* | *destination-addr destination-wildcard* | **any** | **eq** *port* | **gt** *port* | **host** {*address* | *name*} | **lt** *port* | **neq** *port* | **portgroup** *destport-groupname*} [**dscp** *type*] [**fragments**] [**option** *option*] [**precedence** *precedence*] [**log**] [**log-input**] [**time-range** *time-range-name*] [**tos** *tos*]]}

Syntax Description

protocol	Name or number of a protocol; valid values are **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, or **udp**, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP), use the keyword **ip**. See the "Usage Guidelines" section for additional qualifiers.
source-addr	Number of the network or host from which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.
source-wildcard	Wildcard bits to be applied to source in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.
addrgroup *object-group-name*	Specifies the source or destination name of the object group.
any	Specifies any source or any destination host as an abbreviation for the *source-addr* or *destination-addr* value and the *source-wildcard* or *destination-wildcard* value of 0.0.0.0 255.255.255.255.
host *address*	Specifies the source or destination address of a single host.
host *name*	Specifies the source or destination name of a single host.
tcp	Specifies the TCP protocol.
udp	Specifies the UDP protocol.

addrgroup *source-addr-group-name*	Specifies the source address group name.
destination-addr	Number of the network or host to which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.
destination-wildcard	Wildcard bits to be applied to the destination in a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.
eq *port*	Matches only packets on a given port number; see the "Usage Guidelines" section for valid values.
gt *port*	Matches only the packets with a greater port number; see the "Usage Guidelines" section for valid values.
lt *port*	Matches only the packets with a lower port number; see the "Usage Guidelines" section for valid values.
neq *port*	Matches only the packets that are not on a given port number; see the "Usage Guidelines" section for valid values.
portgroup *srcport-group-name*	Specifies the source port object group name.
addrgroup *dest-addr-group-name*	Specifies the destination address group name.
portgroup *destport-group-name*	Specifies the destination port object group name.
dscp *type*	(Optional) Matches the packets with the given Differentiated Services Code Point (DSCP) value; see the "Usage Guidelines" section for valid values.
fragments	(Optional) Applies the access list entry to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the "Access List Processing of Fragments" and "Fragments and Policy Routing" sections in the "Usage Guidelines" section.
option *option*	(Optional) Matches the packets with the given IP options value number; see the "Usage Guidelines" section for valid values.
precedence *precedence*	(Optional) Specifies the precedence filtering level for packets; valid values are a number from 0 to 7 or by a name. See the "Usage Guidelines" sectionfor a list of valid names.

log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message for a standard list includes the access list number, whether the packet was permitted or denied, the source address, and the number of packets. The message for an extended list includes the access list number; whether the packet was permitted or denied; the protocol; whether the protocol was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. For both standard and extended lists, the message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from reloading due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.
log-input	(Optional) Matches the log against this entry, including the input interface.
time-range *time-range-name*	(Optional) Specifies a time-range entry name.
tos *tos*	(Optional) Specifies the service filtering level for packets; valid values are a number from 0 to 15 or by a name as listed in the "Usage Guidelines" section of the **access-list** (IP extended) command.
option *option*	(Optional) Matches packets with the IP options value; see the "Usage Guidelines" section for the valid values.
fragments	(Optional) Applies the access list entry to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the "Access List Processing of Fragments" and "Fragments and Policy Routing" sections in the "Usage Guidelines" section.

Command Default

There is no specific condition under which a packet is denied passing the named access list.

Command Modes

Access-list configuration (config-ext-nacl)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

Use this command following the **ip access-list** command to specify conditions under which a packet cannot pass the named access list.

The **portgroup** keyword appears only when you configure an extended ACL

The *address* or *object-group-name* value is created using the **object-group** command.

The **addrgroup** *object-group-name* keyword and argument allow you to create logical groups of users (or servers), which you can use to define access policy using ACLs. For example, with one ACL entry you can permit the object group named engineering to access all engineering servers. Otherwise, you would need one ACL entry for every person in the engineering group.

If the operator is positioned after the *source-addr* and *source-wildcard* values, it must match the source port.

If the operator is positioned after the *destination-addr* and *destination-wildcard* values, it must match the destination port.

If you are entering the port number of a TCP or UDP port, you can enter the decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the "Usage Guidelines" section of the **access-list** (IP extended) command. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.

The valid values for the **dscp** *type* keyword and argument are as follows:

- **0** to **63**—Differentiated services code point value.
- **af11**—Match packets with AF11 dscp (001010).
- **af12**—Match packets with AF12 dscp (001100).
- **af13**—Match packets with AF13 dscp (001110).
- **af21**—Match packets with AF21 dscp (010010).
- **af22**—Match packets with AF22 dscp (010100).
- **af23**—Matches the patches with the AF23 dscp (010110).
- **af31**—Matches the patches with the AF31 dscp (011010).
- **af32**—Matches the patches with the AF32 dscp (011100).
- **af33**—Matches the patches with the AF33 dscp (011110).
- **af41**—Matches the patches with the AF41 dscp (100010).
- **af42**—Matches the patches with the AF42 dscp (100100).
- **af43**—Matches the patches with the AF43 dscp (100110).
- **cs1**—Matches the patches with the CS1(precedence 1) dscp (001000).
- **cs2**—Matches the patches with the CS2(precedence 2) dscp (010000).
- **cs3**—Matches the patches with the CS3(precedence 3) dscp (011000).
- **cs4**—Matches the patches with the CS4(precedence 4) dscp (100000).
- **cs5**—Matches the patches with the CS5(precedence 5) dscp (101000).
- **cs6**—Matches the patches with the CS6(precedence 6) dscp (110000).
- **cs7**—Matches the patches with the CS7(precedence 7) dscp (111000).
- **default**—Matches the patches with the default dscp (000000).
- **ef**—Matches the patches with the EF dscp (101110).

The valid values for the **eq** *port* keyword and argument are as follows:

- **0** to **65535**—Port number.
- **bgp**—Border Gateway Protocol (179).

- **chargen**—Character generator (19).
- **cmd**—Remote commands (rcmd, 514).
- **daytime**—Daytime (13).
- **discard**—Discard (9).
- **domain**—Domain Name Service (53).
- **echo**—Echo (7).
- **exec**—Exec (rsh, 512).
- **finger**—Finger (79).
- **ftp**—File Transfer Protocol (21).
- **ftp-data**—FTP data connections (20).
- **gopher**—Gopher (70).
- **hostname**—NIC hostname server (101).
- **ident**—Ident Protocol (113).
- **irc**—Internet Relay Chat (194).
- **klogin**—Kerberos login (543).
- **kshell**—Kerberos shell (544).
- **login**—Login (rlogin, 513).
- **lpd**—Printer service (515).
- **nntp**—Network News Transport Protocol (119).
- **pim-auto-rp**—PIM Auto-RP (496).
- **pop2**—Post Office Protocol v2 (109).
- **pop3**—Post Office Protocol v3 (110).
- **smtp**—Simple Mail Transport Protocol (25).
- **sunrpc**—Sun Remote Procedure Call (111).
- **syslog**—Syslog (514).
- **tacacs**—TAC Access Control System (49).
- **talk**—Talk (517).
- **telnet**—Telnet (23).
- **time**—Time (37).
- **uucp**—Unix-to-Unix Copy Program (540).
- **whois**—Nicname (43).
- **www**—World Wide Web (HTTP, 80).

The valid values for the **gt** *port* keyword and argument are as follows:

- **0-65535**—Port number.
- **biff**—Biff (mail notification, comsat, 512).
- **bootpc**—Bootstrap Protocol (BOOTP) client (68).
- **bootps**—Bootstrap Protocol (BOOTP) server (67).
- **discard**—Discard (9).

- **dnsix**—DNSIX security protocol auditing (195).
- **domain**—Domain Name Service (DNS, 53).
- **echo**—Echo (7).
- **isakmp**—Internet Security Association and Key Management Protocol (500).
- **mobile-ip**—Mobile IP registration (434).
- **nameserver**—IEN116 name service (obsolete, 42).
- **netbios-dgm**—NetBios datagram service (138).
- **netbios-ns**—NetBios name service (137).
- **netbios-ss**—NetBios session service (139).
- **non500-isakmp**—Internet Security Association and Key Management Protocol (4500).
- **ntp**—Network Time Protocol (123).
- **pim-auto-rp**—PIM Auto-RP (496).
- **rip**—Routing Information Protocol (router, in.routed, 520).
- **snmp**—Simple Network Management Protocol (161).
- **snmptrap**—SNMP Traps (162).
- **sunrpc**—Sun Remote Procedure Call (111).
- **syslog**—System Logger (514).
- **tacacs**—TAC Access Control System (49).
- **talk**—Talk (517).
- **tftp**—Trivial File Transfer Protocol (69).
- **time**—Time (37).
- **who**—Who service (rwho, 513).
- **xdmcp**—X Display Manager Control Protocol (177).

The valid values for the **lt** *port* keyword and argument are as follows:

- **0**-**65535**—Port number.
- **biff**—Biff (mail notification, comsat, 512).
- **bootpc**—Bootstrap Protocol (BOOTP) client (68).
- **bootps**—Bootstrap Protocol (BOOTP) server (67).
- **discard**—Discard (9).
- **dnsix**—DNSIX security protocol auditing (195).
- **domain**—Domain Name Service (DNS, 53).
- **echo**—Echo (7).
- **isakmp**—Internet Security Association and Key Management Protocol (500).
- **mobile-ip**—Mobile IP registration (434).
- **nameserver**—IEN116 name service (obsolete, 42).
- **netbios-dgm**—NetBios datagram service (138).
- **netbios-ns**—NetBios name service (137).
- **netbios-ss**—NetBios session service (139).

- **non500-isakmp**—Internet Security Association and Key Management Protocol (4500).
- **ntp**—Network Time Protocol (123).
- **pim-auto-rp**—PIM Auto-RP (496).
- **rip**—Routing Information Protocol (router, in.routed, 520).
- **snmp**—Simple Network Management Protocol (161).
- **snmptrap**—SNMP Traps (162).
- sunrpc—Sun Remote Procedure Call (111).
- **syslog**—System Logger (514).
- **tacacs**—TAC Access Control System (49).
- **talk**—Talk (517).
- **tftp**—Trivial File Transfer Protocol (69).
- **time**—Time (37).
- **who**—Who service (rwho, 513).
- **xdmcp**—X Display Manager Control Protocol (177).

The valid values for the **neg** *port* keyword and argument are as follows:

- **0** to **65535**—Port number.
- **biff**—Biff (mail notification, comsat, 512).
- **bootpc**—Bootstrap Protocol (BOOTP) client (68).
- **bootps**—Bootstrap Protocol (BOOTP) server (67).
- **discard**—Discard (9).
- **dnsix**—DNSIX security protocol auditing (195).
- **domain**—Domain Name Service (DNS, 53).
- **echo**—Echo (7).
- **isakmp**—Internet Security Association and Key Management Protocol (500).
- **mobile-ip**—Mobile IP registration (434).
- **nameserver**—IEN116 name service (obsolete, 42).
- **netbios-dgm**—NetBios datagram service (138).
- **netbios-ns**—NetBios name service (137).
- **netbios-ss**—NetBios session service (139).
- **non500-isakmp**—Internet Security Association and Key Management Protoc (4500).
- **ntp**—Network Time Protocol (123).
- **pim-auto-rp**—PIM Auto-RP (496).
- **rip**—Routing Information Protocol (router, in.routed, 520).
- **snmp**—Simple Network Management Protocol (161).
- **snmptrap**—SNMP Traps (162).
- **sunrpc**—Sun Remote Procedure Call (111).
- **syslog**—System Logger (514).
- **tacacs**—TAC Access Control System (49).

- **talk**—Talk (517).
- **tftp**—Trivial File Transfer Protocol (69).
- **time**—Time (37).
- **who**—Who service (rwho, 513).
- **xdmcp**—X Display Manager Control Protocol (177).

The valid values for the **option** *option* keyword and argument are as follows:

- **0** to **255**—IP Options value.
- **add-ext**—Matches the packets with Address Extension Option (147).
- **any-options**—Matches the packets with ANY Option.
- **com-security**—Matches the packets with Commercial Security Option (134).
- **dps**—Matches the packets with Dynamic Packet State Option (151).
- **encode**—Matches the packets with Encode Option (15).
- **eool**—Matches the packets with End of Options (0).
- **ext-ip**—Matches the packets with the Extended IP Option (145).
- **ext-security**—Matches the packets with the Extended Security Option (133).
- **finn**—Matches the packets with the Experimental Flow Control Option (205).
  - **imitd**—Matches the packets with IMI Traffic Desriptor Option (144).
  - **lsr**—Matches the packets with Loose Source Route Option (131).
  - **match-all**—Matches the packets if all specified flags are present.
  - **match-any**—Matches the packets if any specified flag is present.
  - **mtup**—Matches the packets with MTU Probe Option (11).
  - **mtur**—Matches the packets with MTU Reply Option (12).
  - **no-op**—Matches the packets with No Operation Option (1).
  - **psh**—Match the packets on the PSH bit.
  - **nsapa**—Matches the packets with NSAP Addresses Option (150).
  - **reflect**—Creates reflexive access list entry.
  - **record-route**—Matches the packets with Record Route Option (7).
  - **rst**—Matches the packets on the RST bit.
  - **router-alert**—Matches the packets with Router Alert Option (148).
  - **sdb**—Matches the packets with Selective Directed Broadcast Option (149).
  - **security**—Matches the packets with Basic Security Option (130).
  - **ssr**—Matches the packets with Strict Source Routing Option (137).
  - **stream-id**—Matches the packets with Stream ID Option (136).
  - **syn**—Match the packets on the SYN bit.
- **timestamp**—Matches the packets with the Time Stamp Option (68).
- **traceroute**—Matches the packets with the Trace Route Option (82).
- **ump**—Matches the packets with the Upstream Multicast Packet Option (152).
- **visa**—Matches the packets with the Experimental Access Control Option (142).

- **zsu**—Matches the packets with the Experimental Measurement Option (10).

The valid values for the **tos** *value* keyword and argument are as follows:

- **0** to **15**—Type of service value.
- **max-reliability**—Matches the packets with the maximum reliable ToS (2).
- **max-throughput**—Matches the packets with the maximum throughput ToS (4).
- **min-delay**—Matches the packets with the minimum delay ToS (8).
- **min-monetary-cost**—Matches packets with the minimum monetary cost ToS (1).
- **normal**—Matches the packets with the normal ToS (0).

Access List Processing of Fragments

The behavior of access-list entries regarding the use or lack of the **fragments** keyword are summarized in Table 29:

Table 30 Access list Processing of Fragments

If the Access-List Entry Has...	Then...
...no **fragments** keyword (the default behavior), and assuming all of the access-list entry information matches,	For an access-list entry containing only Layer 3 information: • The entry is applied to nonfragmented packets, initial fragments, and noninitial fragments. For an access list entry containing Layer 3 and Layer 4 information: • The entry is applied to nonfragmented packets and initial fragments: – If the entry is a **permit** statement, the packet or fragment is permitted. – If the entry is a **deny** statement, the packet or fragment is denied. • The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access-list entry can be applied. If the Layer 3 portion of the access-list entry matches, and – If the entry is a **permit** statement, the noninitial fragment is permitted. – If the entry is a **deny** statement, the next access-list entry is processed. **Note** The **deny** statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.
...the **fragments** keyword, and assuming all of the access-list entry information matches,	**Note** The access-list entry is applied only to noninitial fragments.The **fragments** keyword cannot be configured for an access-list entry that contains any Layer 4 information.

Be aware that you should not simply add the **fragments** keyword to every access list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments** keyword, the packet is compared to the next access list entry, and so on, until it is either permitted or denied by an access list entry that does not contain the **fragments** keyword. Therefore, you may need two access list entries for every **deny** entry. The first **deny** entry of the pair will not include the **fragments** keyword, and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases where there are multiple **deny** access-list entries for the same host but with different Layer 4 ports, a single **deny** access-list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets and each counts individually as a packet in access list accounting and access list violation counts.

Note The **fragments** keyword cannot solve all cases involving access lists and IP fragments.

Fragments and Policy Routing

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip address** command and the access list had entries that match on Layer 4 through 7 information. It is possible that noninitial fragments pass the access list and are policy routed, even if the first fragment was not policy routed or the reverse.

By using the **fragments** keyword in access list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made and it is more likely policy routing will occur as intended.

The **portgroup** *srcport-groupname or* **portgroup** *destport-groupname* keywords and arguments allow you to create an object group based on a source or destination group.

Examples

The following example creates an access list that denies all TCP packets:

```
Router(config)# ip access-list extended my-pbacl-policy
Router(config-ext-nacl)# deny tcp any any
Router(config-ext-nacl)# exit
Router(config)# exit
```

Related Commands

Command	Description
ip access-group	Controls access to an interface.
ip access-list	Defines an IP access list by name.
logging console	Limits messages logged to the console based on severity.
object-group	Defines object groups to optimize your configuration
permit (Catalyst 6500 series switches)	Sets conditions for a named IP access list.
show ip access-lists	Displays the contents of all current IP access lists.

deny (IP)

To set conditions in a named IP access list that will deny packets, use the **deny** command in access list configuration mode. To remove a deny condition from an access list, use the **no** form of this command.

[*sequence-number*] **deny** *source* [*source-wildcard*]

[*sequence-number*] **deny** *protocol source source-wildcard destination destination-wildcard* [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**log**] [**time-range** *time-range-name*] [**fragments**]

no *sequence-number*

no deny *source* [*source-wildcard*]

no deny *protocol source source-wildcard destination destination-wildcard*

Internet Control Message Protocol (ICMP)

[*sequence-number*] **deny icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* [*icmp-code*] | *icmp-message*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**log**] [**time-range** *time-range-name*] [**fragments**]

Internet Group Management Protocol (IGMP)

[*sequence-number*] **deny igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**log**] [**time-range** *time-range-name*] [**fragments**]

Transmission Control Protocol (TCP)

[*sequence-number*] **deny tcp** *source source-wildcard* [*operator port* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established** | {**match-any** | **match-all**} {**+** | **-**} *flag-name*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**log**] [**time-range** *time-range-name*] [**fragments**]

User Datagram Protocol (UDP)

[*sequence-number*] **deny udp** *source source-wildcard* [*operator port* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**log**] [**time-range** *time-range-name*] [**fragments**]

Syntax Description

sequence-number	(Optional) Sequence number assigned to the deny statement. The sequence number causes the system to insert the statement in that numbered position in the access list.
source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
source-wildcard	Wildcard bits to be applied to the source. There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part dotted-decimal format. Place 1s in the bit positions that you want to ignore. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
protocol	Name or number of an Internet protocol. The *protocol* argument can be one of the keywords **eigrp**, **gre**, **icmp**, **igmp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, or **udp**, or an integer in the range from 0 to 255 representing an Internet protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the **ip** keyword. **Note** When the **icmp**, **igmp**, **tcp,** and **udp** keywords are entered, they must be followed with the specific command syntax that is shown for the ICMP, IGMP, TCP, and UDP forms of the **deny** command.
icmp	Denies only ICMP packets. When you enter the **icmp** keyword, you must use the specific command syntax shown for the ICMP form of the **deny** command.
igmp	Denies only IGMP packets. When you enter the **igmp** keyword, you must use the specific command syntax shown for the IGMP form of the **deny** command.
tcp	Denies only TCP packets. When you enter the **tcp** keyword, you must use the specific command syntax shown for the TCP form of the **deny** command.
udp	Denies only UDP packets. When you enter the **udp** keyword, you must use the specific command syntax shown for the UDP form of the **deny** command.
destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.

destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part dotted-decimal format. Place 1s in the bit positions that you want to ignore. • Use the **any** keyword as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
option *option-name*	(Optional) Packets can be filtered by IP Options, as specified by a number from 0 to 255 or by the corresponding IP Option name, as listed in Table 31 in the "Usage Guidelines" section.
precedence *precedence*	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7 or by a name.
tos *tos*	(Optional) Packets can be filtered by type of service (ToS) level, as specified by a number from 0 to 15, or by a name as listed in the "Usage Guidelines" section of the **access-list** (IP extended) command.
ttl *operator value*	(Optional) Compares the TTL value in the packet to the TTL value specified in this **deny** statement. • The *operator* can be **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), or **range** (inclusive range). • The *value* can range from 0 to 255. • If the operator is **range**, specify two values separated by a space. • For Release 12.0S, if the operator is **eq** or **neq**, only one TTL value can be specified. • For all other releases, if the operator is **eq** or **neq**, as many as 10 TTL values can be specified, separated by a space. If the TTL in the packet matches just one of the possibly 10 values, the entry is considered to be matched.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.)
time-range *time-range-name*	(Optional) Name of the time range that applies to this **deny** statement. The name of the time range and its restrictions are specified by the **time-range** and **absolute** or **periodic** commands, respectively.
fragments	(Optional) The access list entry applies to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the "Access List Processing of Fragments" and "Fragments and Policy Routing" sections in the "Usage Guidelines" section.
icmp-type	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
icmp-code	(Optional) ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.

icmp-message	(Optional) ICMP packets can be filtered by an ICMP message type name or an ICMP message type and code name. The possible names are listed in the "Usage Guidelines" section of the **access-list** (IP extended) command.
igmp-type	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the "Usage Guidelines" section of the **access-list** (IP extended) command.
operator	(Optional) Compares source or destination ports. Operators include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source* and *source-wildcard* arguments, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard* arguments, it must match the destination port. The **range** operator requires two port numbers. Up to ten port numbers can be entered for the **eq** (equal) and **neq** (not equal) operators. All other operators require one port number.
port	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the "Usage Guidelines" section of the **access-list** (IP extended) command. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bit set. The nonmatching case is that of the initial TCP datagram to form a connection. **Note** The **established** keyword can be used only with the old command-line interface (CLI) format. To use the new CLI format, you must use the **match-any** or **match-all** keywords followed by the **+** or **-** keywords and *flag-name* argument.
{**match-any** | **match-all**}	(Optional) For the TCP protocol only: A match occurs if the TCP datagram has certain TCP flags set or not set. You use the **match-any** keyword to allow a match to occur if any of the specified TCP flags are present, or you can use the **match-all** keyword to allow a match to occur only if all of the specified TCP flags are present. You must follow the **match-any** and **match-all** keywords with the **+** or **-** keyword and the *flag-name* argument to match on one or more TCP flags.
{**+** | **-**} *flag-name*	(Optional) For the TCP protocol only: The **+** keyword allows IP packets if their TCP headers contain the TCP flags that are specified by the *flag-name* argument. The **-** keyword filters out IP packets that do not contain the TCP flags specified by the *flag-name* argument. You must follow the **+** and **-** keywords with the *flag-name* argument. TCP flag names can be used only when filtering TCP. Flag names for the TCP flags are as follows: **urg**, **ack**, **psh**, **rst**, **syn**, and **fin**.

Defaults

There are no specific conditions under which a packet is denied passing the named access list.

Command Modes Access list configuration

Command History

Release	Modification
11.2	This command was introduced.
12.0(1)T	The **time-range** *time-range-name* keyword and argument were added.
12.0(11)	The **fragments** keyword was added.
12.2(13)T	The **igrp** keyword was removed because the IGRP protocol is no longer available in Cisco IOS software.
12.2(14)S	The *sequence-number* argument was added.
12.2(15)T	The *sequence-number* argument was added.
12.3(4)T	The **option** *option-name* keyword and argument were added. The **match-any**, **match-all, +**, and **-** keywords and the *flag-name* argument were added.
12.3(7)T	Command functionality was modified to allow up to ten port numbers to be added after the **eq** and **neq** operators so that an access list entry can be created with noncontiguous ports.
12.4(2)T	The **ttl** *operator value* keyword and arguments were added.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines Use this command following the **ip access-list** command to specify conditions under which a packet cannot pass the named access list.

The **time-range** keyword allows you to identify a time range by name. The **time-range**, **absolute**, and **periodic** commands specify when this **deny** statement is in effect.

log Keyword

A log message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval.

Use the **ip access-list log-update** command to generate logging messages when the number of matches reaches a configurable threshold (rather than waiting for a 5-minute-interval). See the **ip access-list log-update** command for more information.

The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing because of too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.

If you enable Cisco Express Forwarding (CEF) and then create an access list that uses the **log** keyword, the packets that match the access list are not CEF-switched. They are fast-switched. Logging disables CEF.

Access List Filtering of IP Options

Access control lists can be used to filter packets with IP Options to prevent routers from being saturated with spurious packets containing IP Options. To see a complete table of all IP Options, including ones currently not in use, refer to the latest Internet Assigned Numbers Authority (IANA) information that is available from its URL: www.iana.org.

Cisco IOS software allows you to filter packets according to whether they contain one or more of the legitimate IP Options by entering either the IP Option value or the corresponding name for the *option-name* argument as shown in Table 31.

Table 31 IP Option Values and Names

IP Option Value or Name	Description
0 to 255	IP Options values.
add-ext	Match packets with Address Extension Option (147).
any-options	Match packets with any IP Option.
com-security	Match packets with Commercial Security Option (134).
dps	Match packets with Dynamic Packet State Option (151).
encode	Match packets with Encode Option (15).
eool	Match packets with End of Options (0).
ext-ip	Match packets with Extended IP Options (145).
ext-security	Match packets with Extended Security Option (133).
finn	Match packets with Experimental Flow Control Option (205).
imitd	Match packets with IMI Traffic Descriptor Option (144).
lsr	Match packets with Loose Source Route Option (131).
mtup	Match packets with MTU Probe Option (11).
mtur	Match packets with MTU Reply Option (12).
no-op	Match packets with No Operation Option (1).
nsapa	Match packets with NSAP Addresses Option (150).
psh	Matches the packets on the PSH bit.
record-route	Match packets with Router Record Route Option (7).
reflect	Creates reflexive access list entry.
rst	Matches the packets on the RST bit.
router-alert	Match packets with Router Alert Option (148).
sdb	Match packets with Selective Directed Broadcast Option (149).
security	Match packets with Base Security Option (130).
ssr	Match packets with Strict Source Routing Option (137).
stream-id	Match packets with Stream ID Option (136).
syn	Matches the packets on the SYN bit.
timestamp	Match packets with Time Stamp Option (68).

Filtering IP Packets Based on TCP Flags

The access list entries that make up an access list can be configured to detect and drop unauthorized TCP packets by allowing only the packets that have very specific groups of TCP flags set or not set. Users can select any desired combination of TCP flags with which to filter TCP packets. Users can configure access list entries in order to allow matching on a flag that is set and on a flag that is not set. Use the **+** and **-** keywords with a flag name to specify that a match is made based on whether a TCP header flag has been set. Use the **match-any** and **match-all** keywords to allow the packet if any or all, respectively, of the flags specified by the **+** or **-** keyword and *flag-name* argument have been set or not set.

Access List Processing of Fragments

The behavior of access list entries regarding the use or lack of use of the **fragments** keyword can be summarized as follows:

If the Access-List Entry Has...	Then...
...no **fragments** keyword (the default behavior), and assuming all of the access-list entry information matches,	For an access list entry that contains only Layer 3 information: • The entry is applied to nonfragmented packets, initial fragments, and noninitial fragments. For an access list entry that contains Layer 3 and Layer 4 information: • The entry is applied to nonfragmented packets and initial fragments. – If the entry is a **permit** statement, then the packet or fragment is permitted. – If the entry is a **deny** statement, then the packet or fragment is denied. • The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access list entry can be applied. If the Layer 3 portion of the access list entry matches, and – If the entry is a **permit** statement, then the noninitial fragment is permitted. – If the entry is a **deny** statement, then the next access list entry is processed. **Note** The **deny** statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.
...the **fragments** keyword, and assuming all of the access-list entry information matches,	The access list entry is applied only to noninitial fragments. The **fragments** keyword cannot be configured for an access list entry that contains any Layer 4 information.

Be aware that you should not add the **fragments** keyword to every access list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments** keyword. The packet is compared to the next access list entry, and so on, until it is either permitted or denied by an access list entry that does not contain the **fragments** keyword. Therefore, you may need two access list entries for every **deny** entry. The first **deny** entry of the pair will not include

the **fragments** keyword and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases in which there are multiple **deny** access list entries for the same host but with different Layer 4 ports, a single **deny** access list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets, and each counts individually as a packet in access list accounting and access list violation counts.

Note The **fragments** keyword cannot solve all cases that involve access lists and IP fragments.

Fragments and Policy Routing

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip address** command and the access list has entries that match on Layer 4 through 7 information. It is possible that noninitial fragments pass the access list and are policy-routed, even if the first fragment is not policy-routed.

By using the **fragments** keyword in access list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made, and it is more likely that policy routing will occur as intended.

Creating an Access List Entry with Noncontiguous Ports

For Cisco IOS Release 12.3(7)T and later releases, you can specify noncontiguous ports on the same access control entry, which greatly reduces the number of access list entries required for the same source address, destination address, and protocol. If you maintain large numbers of access list entries, we recommend that you consolidate them when possible by using noncontiguous ports. You can specify up to ten port numbers following the **eq** and **neq** operators.

Examples

The following example sets conditions for a standard access list named Internetfilter:

```
ip access-list standard Internetfilter
 deny 192.168.34.0  0.0.0.255
 permit 172.16.0.0  0.0.255.255
 permit 10.0.0.0  0.255.255.255
! (Note: all other access implicitly denied.)
```

The following example denies HTTP traffic on Monday through Friday from 8:00 a.m. to 6:00 p.m.:

```
time-range no-http
 periodic weekdays 8:00 to 18:00
!
ip access-list extended strict
 deny tcp any any eq http time-range no-http
!
interface ethernet 0
 ip access-group strict in
```

The following example adds an entry with the sequence number 25 to extended IP access list 150:

```
ip access-list extended 150
 25 deny ip host 172.16.3.3 host 192.168.5.34
```

The following example removes the entry with the sequence number 25 from the extended access list example shown above:

```
 no 25
```

The following example sets a deny condition for an extended access list named filter2. The access list entry specifies that a packet cannot pass the named access list if it contains the Strict Source Routing IP Option, which is represented by the IP option value ssr.

```
ip access-list extended filter2
 deny ip any any option ssr
```

The following example sets a deny condition for an extended access list named kmdfilter1. The access list entry specifies that a packet cannot pass the named access list if the RST and FIN TCP flags have been set for that packet:

```
ip access-list extended kmdfilter1
 deny tcp any any match-any +rst +fin
```

The following example shows several **deny** statements that can be consolidated into one access list entry with noncontiguous ports. The **show access-lists** command is entered to display a group of access list entries for the access list named abc.

```
Router# show access-lists abc

Extended IP access list abc
 10 deny tcp any eq telnet any eq 450
 20 deny tcp any eq telnet any eq 679
 30 deny tcp any eq ftp any eq 450
 40 deny tcp any eq ftp any eq 679
```

Because the entries are all for the same **deny** statement and simply show different ports, they can be consolidated into one new access list entry. The following example shows the removal of the redundant access list entries and the creation of a new access list entry that consolidates the previously displayed group of access list entries:

```
ip access-list extended abc
 no 10
 no 20
 no 30
 no 40
 deny tcp any eq telnet ftp any eq 450 679
```

The following examples shows the creation of the consolidated access list entry:

```
Router# show access-lists abc

Extended IP access list abc
 10 deny tcp any eq telnet ftp any eq 450 679
```

The following access list filters IP packets containing Type of Service (ToS) level 3 with TTL values 10 and 20. It also filters IP packets with a TTL greater than 154 and applies that rule to noninitial fragments. It permits IP packets with a precedence level of flash and a TTL not equal to 1, and sends log messages about such packets to the console. All other packets are denied.

```
ip access-list extended canton
 deny ip any any tos 3 ttl eq 10 20
 deny ip any any ttl gt 154 fragments
 permit ip any any precedence flash ttl neq 1 log
```

Related Commands

Command	Description
absolute	Specifies an absolute time when a time range is in effect.
access-list (IP extended)	Defines an extended IP access list.

Command	Description
access-list (IP standard)	Defines a standard IP access list.
ip access-group	Controls access to an interface.
ip access-list	Defines an IP access list by name.
ip access-list log-update	Sets the threshold number of packets that cause a logging message.
ip access-list resequence	Applies sequence numbers to the access list entries in an access list.
ip options	Drops or ignores IP Options packets that are sent to the router.
logging console	Sends system logging (syslog) messages to all available TTY lines and limits messages based on severity.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, or performs policy routing on packets.
periodic	Specifies a recurring (weekly) time range for functions that support the time-range feature.
permit (IP)	Sets conditions under which a packet passes a named IP access list.
remark	Writes a helpful comment (remark) for an entry in a named IP access list.
show access-lists	Displays a group of access-list entries.
show ip access-list	Displays the contents of all current IP access lists.
time-range	Specifies when an access list or other feature is in effect.

deny (MAC ACL)

To set conditions for a MAC access list, use the **deny** command in MAC access-list extended configuration mode. To remove a condition from an access list, use the **no** form of this command.

deny {*src_mac_mask* | {**host name** *src_mac_name*} | **any**} {*dest_mac_mask* | {**host name** *dst_mac_name*} | **any**} [{*protocol_keyword* | {*ethertype_number ethertype_mask*}} [**vlan** *vlan_ID*] [**cos** *cos_value*]]

no deny {*src_mac_mask* | {**host name** *src_mac_name*} | **any**} {*dest_mac_mask* | {**host name** *dst_mac_name*} | **any**} [{*protocol_keyword* | {*ethertype_number ethertype_mask*}} [**vlan** *vlan_ID*] [**cos** *cos_value*]]

Syntax Description

src_mac_mask	Specifies the MAC address mask that identifies a selected block of source MAC addresses. A value of 1 represents a wildcard in that position.
host name *src_mac_name*	Specifies a source host that has been named using the **mac host name** command.
any	Specifies any source or any destination host as an abbreviation for the *src_mac_mask* or *dest_mac_mask* value of 1111.1111.1111, which declares all digits to be wildcards.
dest_mac_mask	Specifies the MAC address mask that identifies a selected block of destination MAC addresses.
host name *dst_mac_name*	Specifies a destination host that has been named using the **mac host name** command.
protocol_keyword	(Optional) Specifies a named protocol (for example, ARP).
ethertype_number	(Optional) The EtherType number specifies the protocol within the Ethernet packet.
ethertype_mask	(Optional) The EtherType mask allows a range of EtherTypes to be specified together. This is a hexadecimal number from 0 to FFFF. An EtherType mask of 0 requires an exact match of the EtherType.
vlan *vlan_ID*	(Optional) Specifies a VLAN.
cos *cos_value*	(Optional) Specifies the Layer 2 priority level for packets. The range is from 0 to 7.

Command Default

This command has no defaults.

Command Modes

MAC access-list extended configuration (config-ext-macl)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

Use this command following the **ip access-list** command to define the conditions under which a packet passes the access list.

- The **vlan** and **cos** keywords are not supported in MAC ACLs used for VACL filtering.
- The **vlan** keyword for VLAN-based QoS filtering in MAC ACLs can be globally enabled or disabled and is disabled by default.
- Enter MAC addresses as three 2-byte values in dotted hexadecimal format. For example, 0123.4567.89ab.
- Enter MAC address masks as three 2-byte values in dotted hexadecimal format. Use 1 bits as wildcards. For example, to match an address exactly, use 0000.0000.0000 (can be entered as 0.0.0).
- An entry without a protocol parameter matches any protocol.
- Enter an EtherType and an EtherType mask as hexadecimal values from 0 to FFFF.
- This list shows the EtherType values and their corresponding protocol keywords:
  - 0x0600—xns-idp—Xerox XNS IDP
  - 0x0BAD—vines-ip—Banyan VINES IP
  - 0x0baf—vines-echo—Banyan VINES Echo
  - 0x6000—etype-6000—DEC unassigned, experimental
  - 0x6001—mop-dump—DEC Maintenance Operation Protocol (MOP) Dump/Load Assistance
  - 0x6002—mop-console—DEC MOP Remote Console
  - 0x6003—decnet-iv—DEC DECnet Phase IV Route
  - 0x6004—lat—DEC Local Area Transport (LAT)
  - 0x6005—diagnostic—DEC DECnet Diagnostics
  - 0x6007—lavc-sca—DEC Local-Area VAX Cluster (LAVC), SCA
  - 0x6008—amber—DEC AMBER
  - 0x6009—mumps—DEC MUMPS
  - 0x0800—ip—Malformed, invalid, or deliberately corrupt IP frames
  - 0x8038—dec-spanning—DEC LANBridge Management
  - 0x8039—dsm—DEC DSM/DDP
  - 0x8040—netbios—DEC PATHWORKS DECnet NETBIOS Emulation
  - 0x8041—msdos—DEC Local Area System Transport
  - 0x8042—etype-8042—DEC unassigned
  - 0x809B—appletalk—Kinetics EtherTalk (AppleTalk over Ethernet)
  - 0x80F3—aarp—Kinetics AppleTalk Address Resolution Protocol (AARP)

Examples

This example shows how to create a MAC-Layer ACL named mac_layer that denies dec-phase-iv traffic with source address 0000.4700.0001 and destination address 0000.4700.0009, but allows all other traffic:

```
Router(config)# mac access-list extended mac_layer
Router(config-ext-macl)# deny 0000.4700.0001 0.0.0 0000.4700.0009 0.0.0 dec-phase-iv
Router(config-ext-macl)# permit any any
```

Related Commands

Command	Description
permit (MAC ACL)	Sets permit conditions for a named MAC access list.
mac access-list extended	Defines a MAC access list by name.
mac host	Assigns a name to a MAC address.
show mac access-group	Displays the contents of all current MAC access groups.

deny (WebVPN)

To set conditions in a named Secure Sockets Layer Virtual Private Network (SSL VPN) access list that will deny packets, use the **deny** command in webvpn acl configuration mode. To remove a deny condition from an access list, use the **no** form of this command.

deny [**url** [**any** | *url-string*]] [**ip** | **tcp** | **udp** | **http** | **https** | **cifs**] [**any** | *source-ip source-mask*] [**any** | *destination-ip destination-mask*] [**time-range** *time-range-name*] [**syslog**]

no deny url [**any** | *url-string*] [**ip** | **tcp** | **udp** | **http** | **https** | **cifs**] [**any** | *source-ip source-mask*] [**any** | *destination-ip destination-mask*] [**time-range** *time-range-name*] [**syslog**]

Syntax Description

url	(Optional) Filtering rules are applied to the URL. • Use the **any** keyword as an abbreviation for any URL.
url-string	(Optional) URL string defined as follows: **scheme://host[:port][/path]** • **scheme**—Can be HTTP, Secure HTTPS (HTTPS), or Common Internet File System (CIFS). This field is required in the URL string. • **host**—Can be a hostname or a host IP (host mask). The host can have one wildcard (*). • **port**—Can be any valid port number (1–65535). It is possible to have multiple port numbers separated by a comma (,). The port range is expressed using a dash (-). • **path**—Can be any valid path string. In the path string, the $user is translated to the current user name.
ip	(Optional) Denies only IP packets. When you enter the **ip** keyword, you must use the specific command syntax shown for the IP form of the deny command.
tcp	(Optional) Denies only TCP packets. When you enter the **tcp** keyword, you must use the specific command syntax shown for the TCP form of the deny command.
udp	(Optional) Denies only UDP packets. When you enter the **udp** keyword, you must use the specific command syntax shown for the UDP form of the deny command.
http	(Optional) Denies only HTTP packets. When you enter the **http** keyword, you must use the specific command syntax shown for the HTTP form of the deny command.
https	(Optional) Denies only HTTPS packets. When you enter the **https** keyword, you must use the specific command syntax shown for the HTTPS form of the deny command.
cifs	(Optional) Denies only CIFS packets. When you enter the **cifs** keyword, you must use the specific command syntax shown for the CIFS form of the deny command.
source-ip source-mask	(Optional) Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for a source and source mask of 0.0.0.0 255.255.255.255. • Use **host** source as an abbreviation for a source and source-wildcard of source 0.0.0.0.

destination-ip destination-mask	(Optional) Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for a source and source mask of 0.0.0.0 255.255.255.255. • Use **host** source as an abbreviation for a source and source-wildcard of source 0.0.0.0.
time-range *time-range-name*	(Optional) Name of the time range that applies to this **deny** statement. The name of the time range and its restrictions are specified by the **time-range** and **absolute** or **periodic** commands, respectively.
syslog	(Optional) System logging messages are generated.

Command Default

There are no specific conditions under which a packet is denied passing the named access list.

Command Modes

Webvpn acl configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use this command following the **acl** command to specify conditions under which a packet cannot pass the named access list.

The **time-range** keyword allows you to identify a time range by name. The **time-range**, **absolute**, and **periodic** commands specify when this deny statement is in effect.

Examples

The following example shows that all packets from the URL "https://10.168.2.228:34,80-90,100-/public" will be denied:

```
webvpn context context1
 acl acl1
  deny url "https://10.168.2.228:34,80-90,100-/public"
```

Related Commands

Command	Description
absolute	Specifies an absolute time for a time range.
periodic	Specifies a recurring (weekly) time range for functions that support the time-range feature.
permit (webvpn acl)	Sets conditions to allow a packet to pass a named SSL VPN access list.
time-range	Enables time-range configuration mode and defines time ranges for functions (such as extended access lists).

description (dot1x credentials)

To specify a description for an 802.1X profile, use the **description** command in dot1x credentials configuration mode. To remove the description, use the **no** form of this command.

description *text*

no description

Syntax Description

text	Text description. The description can be up to 80 characters.

Command Default

A description is not specified.

Command Modes

Dot1x credentials configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Before using this command, the **dot1x credentials** command must have been configured.

An 802.1X credential structure is necessary when configuring a supplicant (client). This credentials structure may contain a username, password, and description.

Examples

The following example shows which credentials profile should be used when configuring a supplicant, and it provides a description of the credentials profile:

```
dot1x credentials basic-user
 username router
 password secret
 description This credentials profile should be used for most configured ports
```

The credentials structure can be applied to an interface, along with the **dot1x pae supplicant** command and keyword, to enable supplicant functionality on that interface.

```
interface fastethernet 0/1
 dot1x credentials basic-user
 dot1x pae supplicant
```

Related Commands

Command	Description
dot1x credentials	Specifies which 802.1X credentials profile to use.

description (identify zone)

To enter a description of a zone, use the **description** command in security zone configuration mode. To remove the description of the zone, use the **no** form of this command.

description *line-of-description*

no description *line-of-description*

Syntax Description

line-of-description	Description of the zone. You can enter up to 40 characters.

Command Default

None

Command Modes

Security zone configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use this subcommand after entering the **zone security** or **zone-pair security** command.

Examples

The following example specifies that zone z1 is a testzone:

```
zone security z1
 description testzone
```

Related Commands

Command	Description
zone-pair security	Creates a zone-pair that is the type security.
zone security	Creates a zone.

description (identity policy)

To enter a description for an identity policy, use the **description** command in identity policy configuration mode. To remove the description, use the **no** form of this command.

description *line-of-description*

no description *line-of-description*

Syntax Description

line-of-description	Description of the identity policy.

Defaults

A description is not entered for the identity policy.

Command Modes

Identity policy configuration (config-identity-policy)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Examples

The following example shows that a default identity policy and its description ("policyname1") have been specified:

```
Router (config)# identity policy policyname1
Router (config-identity-policy)# description policyABC
```

Related Commands

Command	Description
description (identity profile)	Enters a description for an identity profile.

description (identity profile)

To enter a description for an identity profile, use the **description** command in identity profile configuration mode. To remove the description of the identity profile, use the **no** form of this command.

description *line-of-description*

no description *line-of-description*

Syntax Description

line-of-description	Description of the identity profile.

Defaults

A description is not entered for the identity profile.

Command Modes

Identity profile configuration (config-identity-prof)

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(8)T	This command was previously configured in dot1x configuration mode.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

The **identity profile** command and one of its keywords (**default**, **dot1x**, or **eapoudp**) must be entered in global configuration mode before the **description** command can be used.

Examples

The following example shows that a default identity profile and its description (“ourdefaultpolicy”) have been specified:

```
Router (config)# identity profile default
Router (config-identity-prof)# description ourdefaultpolicy
```

Related Commands

Command	Description
description (identity policy)	Enters a description for an identity policy.
identity profile	Creates an identity profile and enters identity profile configuration mode.

description (IKEv2 keyring)

To add the description of an Internet Key Exchange Version 2 (IKEv2) peer or profile, use the **description** command in the IKEv2 keyring peer configuration mode. To delete the description, use the **no** form of this command.

description *line-of-description*

no description *line-of-description*

Syntax Description

line-of-description	Description given to an IKE peer or profile.

Command Default

The peer or profile is not described.

Command Modes

IKEv2 keyring peer configuration (config-ikev2-keyring-peer)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to provide a descriptive line about the IKEv2 peer, peer group, or profile.

Examples

The following example shows that the description "connection from site A" has been added to an IKEv2 peer:

```
Router(config)# crypto ikev2 keyring keyr 1
Router(configikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# description connection from site A
```

Related Commands

Command	Description
address (ikev2 keyring)	Specifies the IPv4 address or the range of the peers in IKEv2 keyring.
crypto ikev2 keyring	Defines an IKEv2 keyring.
hostname (ikev2 keyring)	Specifies the hostname for the peer in the IKEv2 keyring.
identity (ikev2 keyring)	Identifies the peer with IKEv2 types of identity.

Command	Description
peer	Defines a peer or a peer group for the keyring.
pre-shared-key (ikev2 keyring)	Defines a preshared key for the IKEv2 peer.

description (isakmp peer)

To add the description of an Internet Key Exchange (IKE) peer, use the **description** command in ISAKMP peer configuration mode. To delete the description, use the **no** form of this command.

description *line-of-description*

no description *line-of-description*

Syntax Description

line-of-description	Description given to an IKE peer.

Defaults

No default behavior or values

Command Modes

ISAKMP peer configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.

Usage Guidelines

IKE peers that "sit" behind a Network Address Translation (NAT) device cannot be uniquely identified; therefore, they have to share the same peer description.

Examples

The following example shows that the description "connection from site A" has been added for an IKE peer:

```
Router# crypto isakmp peer address 10.2.2.9
Router (config-isakmp-peer)# description connection from site A
```

Related Commands

Command	Description
clear crypto session	Deletes crypto sessions (IPSec and IKE SAs).
show crypto isakmp peer	Displays peer descriptions.
show crypto session	Displays status information for active crypto sessions in a router.

destination host

To configure the fully qualified domain name (FQDN) of a Diameter peer, use the **destination host** command in diameter peer configuration submode. To disable the configured FQDN, use the **no** form of this command.

destination host *string*

no destination host *string*

Syntax Description

string	The FQDN of the Diameter peer.

Command Default

No FQDN is configured.

Command Modes

Diameter peer configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Examples

The following example shows how to configure the destination host:

```
Router(config-dia-peer)# destination host host1.example.com.
```

Related Commands

Command	Description
destination realm	Configures the destination realm of a Diameter peer.
diameter peer	Configures a Diameter peer and enters Diameter peer configuration submode.

destination realm

To configure the destination realm of a Diameter peer, use the **destination realm** command in diameter peer configuration submode. To disable the configured realm, use the **no** form of this command.

destination realm *string*

no destination realm *string*

Syntax Description

string	The destination realm (part of the domain @*realm*) in which a Diameter peer is located.

Command Default

No realm is configured.

Command Modes

Diameter peer configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

The realm might be added by the authentication, authorization, and accounting (AAA) client when sending a request to AAA. However, if the client does not add the attribute, then the value configured while in Diameter peer configuration submode is used when sending messages to the destination Diameter peer. If a value is not configured while in Diameter peer configuration submode, the value specified by the **diameter destination realm** global configuration command is used.

Examples

The following example shows how to configure the destination realm:

```
router (config-dia-peer)# destination realm example.com
```

Related Commands

Command	Description
diameter destination realm	Configures a global Diameter destination realm.
diameter peer	Configures a Diameter peer and enters Diameter peer configuration submode.

device (identity profile)

To statically authorize or reject individual devices, use the **device** command in identity profile configuration mode. To disable the authorization or rejection, use the **no** form of this command.

device {**authorize** {**ip address** *ip-address* **policy** *policy-name* | **mac-address** *mac-address* | **type** {**cisco** | **ip** | **phone**}} | **not-authorize**}

no device {**authorize** {**ip address** *ip-address* **policy** *policy-name* | **mac-address** *mac-address* | **type** {**cisco** | **ip** | **phone**}} | **not-authorize**}

Syntax Description

authorize	Configures an authorized device.
ip address	Specifies a device by its IP address.
ip-address	The IP address.
policy	Applies an associated policy with the device.
policy-name	Name of the policy.
mac-address	Specifies a device by its MAC address.
mac-address	The MAC address.
type	Specifies a device by its type.
cisco	Specifies a Cisco device.
ip	Specifies an IP device.
phone	Specifies a Cisco IP phone.
not-authorize	Configures an unauthorized device.

Defaults

A device is not statically authorized or rejected.

Command Modes

Identity profile configuration (config-identity-prof)

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(8)T	The **unauthorize** keyword was changed to **not authorize**. The *cisco-device* argument was deleted. The **ip address** keyword and *ip-address* argument were added. The **ip** and **phone** keywords were added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

The **identity profile** command and **default**, **dot1x**, or **eapoudp** keywords must be entered in global configuration mode before the **device** command can be used.

Examples

The following configuration example defines an identity profile for Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) to statically authorize host 192.168.1.3 with "policyname1" as the associated identity policy:

```
Router(config)# identity profile eapoudp
Router(config-identity-prof)# device authorize ip-address 192.168.1.3 policy policyname1
```

Related Commands

Command	Description
identity profile eapoudp	Creates an identity profile.

dhcp (IKEv2)

To assign an IP address to the remote access client using a DHCP server, use the **dhcp** command in IKEv2 authorization policy configuration mode. To remove the assigned IP address, use the **no** form of this command.

dhcp {**giaddr** *ip-address* | **server** {*ip-address* | *hostname*} | **timeout** *seconds*}

no dhcp {**giaddr** | **server** | **timeout**}

Syntax Description

giaddr *ip-address*	Specifies the gateway IP address (giaddr).
server	Specifies addresses for the DHCP server.
ip-address	IP address of the DHCP server.
hostname	Hostname of the DHCP server. The hostname is resolved during configuration.
timeout *seconds*	Specifies the wait time in seconds before the next DHCP server in the list is tried.

Command Default

An IP address is not assigned by a DHCP server.

Command Modes

IKEv2 client group configuration (config-ikev2-author-policy)

Command History

Release	Modification
15.1(3)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

If this command is not configured, an IP address is assigned to a remote device using either a local pool that is configured on a router or a framed IP address attribute that is defined in RADIUS.

Note You can specify only one DHCP server.

Examples

The following example shows that the IP address of the DHCP server is 192.0.2.1 and that the time to wait until the next DHCP server on the list is tried is 6 seconds:

```
Router(config)# crypto ikev2 authorization policy home
Router(config-ikev2-client-config-group)# key abcd
Router(config-ikev2-client-config-group)# dhcp server 192.0.2.1
Router(config-ikev2-client-config-group)# dhcp timeout 6
```

Related Commands

Command	Description
crypto ikev2 authorization policy	Specifies an IKEv2 authorization policy group.

dhcp server (isakmp)

To assign an IP address or hostname using a DHCP server, use the **dhcp server** command in crypto ISAKMP group configuration mode. To remove the assigned IP address or hostname, use the **no** form of this command.

dhcp server {*ip-address* | *hostname*}

no dhcp server {*ip-address* | *hostname*}

Syntax Description

ip-address	Address of the DHCP server.
hostname	Hostname of the DHCP server.

Command Default

IP address is not assigned by a DHCP server.

Command Modes

Crypto ISAKMP group configuration (config-isakmp-group)

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

If this command is not configured, an IP address is assigned to a remote device using either a local pool that is configured on a router or a framed IP address attribute that is defined in RADIUS.

Note Up to five DHCP servers can be configured one at a time.

Note The DHCP proxy feature does not include functionality for the DHCP server to "push" the DNS, WINS server, or domain name to the remote client.

Examples

The following example shows that the IP address of the DHCP server is 10.2.3.4 and that the time to wait until the next DHCP server on the list is tried is 6 seconds:

```
Router (config)# crypto isakmp client configuration group home
 Router (config-isakmp-group)# key abcd
 Router (config-isakmp-group)# dhcp server 10.2.3.4
 Router (config-isakmp-group)# dhcp timeout 6
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.

dhcp timeout

To set the wait time before the next DHCP server on the list is tried, use the **dhcp timeout** command in crypto ISAKMP group configuration mode. To remove the wait time that was set, use the **no** form of this command.

dhcp timeout *time*

no dhcp timeout *time*

Syntax Description

time	Response time in seconds. Value = 4 through 30.

Command Modes

Crypto ISAKMP group configuration (config-isakmp-group)

Command History

Release	Modification
12.4(9)T	This command was introduced.

Examples

The following example shows that the IP address of the DHCP server is 10.2.3.4 and that the time to wait until the next DHCP server on the list is tried is 6 seconds:

```
Router (config)# crypto isakmp client configuration group home
 Router (config-isakmp-group)# dhcp server 10.2.3.4
 Router (config-isakmp-group)# key abcd
 Router (config-isakmp-group)# dhcp timeout 6
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.

dialer aaa

To allow a dialer to access the authentication, authorization, and accounting (AAA) server for dialing information, use the **dialer aaa** command in interface configuration mode. To disable this function, use the **no** form of this command.

dialer aaa [**password** *string* | **suffix** *string*]

no dialer aaa [**password** *string* | **suffix** *string*]

Syntax Description

password *string*	(Optional) Defines a nondefault password for authentication. The password string can be a maximum of 128 characters.
suffix *string*	(Optional) Defines a suffix for authentication. The suffix string can be a maximum of 64 characters.

Defaults

This feature is not enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.1(5)T	The **password** and **suffix** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is required for large scale dial-out and Layer 2 Tunneling Protocol (L2TP) dial-out functionality. With this command, you can specify a suffix, a password, or both. If you do not specify a password, the default password will be "cisco."

Note Only IP addresses can be specified as usernames for the **dialer aaa suffix** command.

Examples

This example shows a user sending out packets from interface Dialer1 with a destination IP address of 10.1.1.1. The username in the access-request message is "10.1.1.1@ciscoDoD" and the password is "cisco."

```
interface dialer1
 dialer aaa
 dialer aaa suffix @ciscoDoD password cisco
```

Related Commands

Command	Description
accept dialout	Accepts requests to tunnel L2TP dial-out calls and creates an accept-dialout VPDN subgroup.
dialer congestion-threshold	Specifies congestion threshold in connected links.
dialer vpdn	Enables a Dialer Profile or DDR dialer to use L2TP dial-out.

diameter origin host

To configure the fully qualified domain name (FQDN) of the host of a Diameter node, use the **diameter origin host** command in global configuration mode. To disable the configured FQDN, use the **no** form of this command.

diameter origin host *string*

no diameter origin host *string*

Syntax Description

string	Character string that describes the FQDN for a specific Diameter node.

Command Default

No realm is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Because there is no host configured by default, it is mandatory to configure this information. The origin host information is sent in requests to a Diameter peer. Global Diameter protocol parameters are used if Diameter parameters have not been defined at a Diameter peer level.

Examples

The following example shows how to configure a Diameter origin host:

```
Router(config)# diameter origin host host1.example.com.
```

Related Commands

Command	Description
diameter origin realm	Configures origin realm information for a Diameter node.
diameter peer	Defines a Diameter peer and enters Diameter peer configuration mode.

diameter origin realm

To configure origin realm information for a Diameter node, use the **diameter origin realm** command in global configuration mode. To disable the configured realm information, use the **no** form of this command.

diameter origin realm *string*

no diameter origin realm *string*

Syntax Description

string	Character string that describes the realm information for a specific Diameter node.

Command Default

No realm is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Because there is no realm configured by default, it is mandatory to configure this information. Origin realm information is sent in requests to a Diameter peer.

Examples

The following example shows how to configure a Diameter origin realm:

```
Router (config)# diameter origin realm example.com
```

Related Commands

Command	Description
diameter origin host	Configures the FQDN of the host of a Diameter node.
diameter peer	Defines a Diameter peer and enters Diameter peer configuration mode.

diameter peer

To configure a device as a Diameter Protocol peer and enter the Diameter peer configuration submode, use the **diameter peer** command in global configuration mode. To disable Diameter Protocol configuration for a peer, use the **no** form of this command.

diameter peer *name*

no diameter peer *name*

Syntax Description

name	Character string used to name the peer node to be configured for the Diameter Credit Control Application (DCCA).

Command Default

No Diameter peer is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command enables the Diameter peer configuration submode. From the submode, you can configure other DCCA parameters. The configuration is applied when you exit the submode.

Examples

The following example shows how to configure a Diameter peer:

```
Router (config)# diameter peer dia_peer_1
```

Related Commands

Command	Description
address ipv4	Defines a route to the host of the Diameter peer using IPv4.
destination host	Configures the FQDN of a Diameter peer.
destination realm	Configures the destination realm in which a Diameter peer is located.
ip vrf forwarding	Associates a VRF with a Diameter peer.
security ipsec	Configures IPSec as the security protocol for the Diameter peer-to-peer connection.
show diameter peer	Displays the Diameter peer configuration.
source interface	Configures the interface to connect to the Diameter peer.
timer	Configures Diameter base protocol timers for peer-to-peer communication.
transport {tcp} port	Configures the transport protocol for connections to the Diameter peer.

diameter redundancy

To enable the Diameter node to be a Cisco IOS Redundancy Facility (RF) client and track session states, use the **diameter redundancy** command in global configuration mode. To disable this feature, use the **no** form of this command.

diameter redundancy

no diameter redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

Diameter redundancy is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

When you configure Diameter redundancy on a device, that device will not initiate any TCP connection while it is a standby node. Upon transition to active status, the device initiates a TCP connection to the Diameter peer.

Note This command is required for service-aware Packet Data Protocol (PDP) session redundancy. For more information about service-aware PDP session redundancy, see the "GTP-Session Redundancy for Service-Aware PDPs Overview" section of the *Cisco GGSN Release 5.2 Configuration Guide*.

Examples

The following example shows how to configure Diameter redundancy:

```
Router (config)# diameter redundancy
```

Related Commands

Command	Description
diameter origin host	Configures the FQDN of the host of this Diameter node.
diameter origin realm	Configures the realm of origin in which this Diameter node is located.
diameter timer	Configures Diameter base protocol timers to use if none have been configured at the Diameter peer level.
diameter vendor support	Configures a Diameter node to advertise the vendor AVPs it supports in capability exchange messages with Diameter peers.

diameter timer

To set either the frequency of transport connection attempts or the interval for sending watchdog messages, use the **diameter timer** command in global configuration mode. To return to the default values, use the **no** form of this command.

diameter timer {**connection** | **transaction** | **watch-dog**} *value*

no diameter timer {**connection** | **transaction** | **watch-dog**} *value*

Syntax Description

connection	Maximum interval, in seconds, for the Gateway General Packet Radio Service (GPRS) Support Node (GGSN) to attempt reconnection to a Diameter peer after being disconnected due to a transport failure. The range is from 1 to 1000. The default is 30. A value of 0 configures the GGSN not to attempt reconnection.
transaction	Maximum interval, in seconds, the GGSN waits for a Diameter peer to respond before trying another peer. The range is from 1 to 1000. The default is 30.
watch-dog	Maximum interval, in seconds, the GGSN waits for a Diameter peer response to a watchdog packet. The range is from 1 to 1000. The default is 30. **Note** When the watchdog timer expires, a device watchdog request (DWR) is sent to the Diameter peer and the watchdog timer is reset. If a device watchdog answer (DWA) is not received before the next expiration of the watchdog timer, a transport failure to the Diameter peer has occurred.
value	The valid range, in seconds, from 1 to 1000. The default is 30.

Command Default

The default value for each timer is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

When configuring timers, the value for the transaction timer should be larger than the transmission-timeout value, and, on the Serving GPRS Support Node (SGSN), the values configured for the number of GPRS Tunneling Protocol (GTP) N3 requests and T3 retransmissions must be larger than the sum of all possible server timers (RADIUS, Diameter Credit Control Application (DCCA), and Cisco Content Services Gateway (CSG)). Specifically, the SGSN N3*T3 must be greater than 2 x RADIUS timeout + *N* x DCCA timeout + CSG timeout where:

- The factor *2* is for both authentication and accounting.
- The value *N* is for the number of Diameter servers configured in the server group.

Examples

The following examples show how to configure the Diameter timers:

```
Router config# diameter timer connection 20

Router config# diameter timer watch-dog 25
```

Related Commands

Command	Description
aaa group server diameter	Defines a Diameter AAA server group.
diameter peer	Configures a Diameter peer and enters Diameter peer configuration submode.
timer	Configures the Diameter base protocol timers for a Diameter peer.

diameter vendor supported

To configure a Diameter node to advertise the vendor-specific attribute value pairs (AVPs) it recognizes, use the **diameter vendor supported** command in global configuration mode. To remove the supported vendor configuration, use the **no** form of this command.

diameter vendor supported {**Cisco** | **3gpp** | **Vodafone**}

no diameter vendor supported {**Cisco** | **3gpp** | **Vodafone**}

Syntax Description

Cisco	Configures the Diameter node to advertise support for the Cisco-specific AVPs.
3gpp	Configures the Diameter node to advertise support for the AVPs that support the Third-Generation Partnership Project (3GPP).
Vodafone	Configures the Diameter node to advertise support for the Vodafone-specific AVPs.

Command Default

No vendor identifier is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Individual vendors can define AVPs specific to their implementation of the Diameter Credit Control Application (DCCA), or for individual applications. You can configure multiple instances of this command, as long as each instance has a different vendor identifier.

Examples

The following example shows how to configure DCCA to advertise support for a the Cisco-specific AVPs:

```
Router (config)# diameter vendor supported Cisco
```

Related Commands

Command	Description
diameter origin host	Configures the FQDN of the host of this Diameter node.
diameter origin realm	Configures the realm of origin in which this Diameter node is located.
diameter redundancy	Enables the Diameter node to be a Cisco IOS RF client and track session states.
diameter timer	Configures Diameter base protocol timers to use if none have been configured at the Diameter peer level.

disable open-media-channel

To prevent the creation of Real-time Transport Protocol (RTP) or RTP Control (RTCP) media channels when a Session Initiation Protocol (SIP) class map is used for SIP inspection, use the **disable open-media-channel** command in parameter-map type configuration mode. To enable the creation of RTP or RTCP media channels, use the **no** form of this command or remove this parameter map from the inspect action.

disable open-media-channel

no disable open-media-channel

Syntax Description

This command has no arguments or keywords.

Command Default

RTP and RTPC media channels are opened by the SIP inspection process.

Command Modes

Parameter-map type configuration (config-profile)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Cisco IOS Firewall Trust Relay Point (TRP) support enables Cisco IOS Firewall to process Simple Traversal of User Datagram Protocol (UDP) (STUN) messages. The STUN messages open ports (pinholes) for secondary channels (RTP and RTCP), which are necessary for implementation of TRPs in voice networks.

Cisco IOS Firewall supports partial SIP inspection that allows the SIP Application-level Gateway (ALG) to parse the SIP message in a packet to check for protocol conformance.

To configure partial SIP inspection in voice networks, you must use the **disable open-media-channel** command to configure SIP ALG so that it does not open pinholes for media information found in the SDP message.

When Cisco IOS TRP is used in voice network for firewall traversal, Partial SIP-ALG (enabled when this parameter map is attached to the inspect action) provides security for SIP control channel and STUN with Cisco Flow data (CFD) provides security for the RTP and RTCP channels. If Partial SIP-ALG is not used, the normal SIP-ALG will open RTP and RTCP channels by itself.

Examples

The following example shows how to create a parameter map that does not open a media channel when attached to a SIP class map:

```
Router(config)# parameter-map type protocol-info sip pmap-sip
Router(config-profile)# disable open-media-channel
```

Related Commands

Command	Description
parameter-map type protocol-info	Creates or modifies a protocol-specific parameter map and enters parameter-map type configuration mode.

disconnect ssh

To terminate a Secure Shell (SSH) connection on your router, use the **disconnect ssh** command in privileged EXEC mode.

disconnect ssh [**vty**] *session-id*

Syntax Description

vty	(Optional) Virtual terminal for remote console access.
session-id	The session-id is the number of connection displayed in the **show ip ssh** command output.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1 T.
12.2(17a)SX	This command was integrated into Cisco IOS Release 12.2(17a)SX.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

The **clear line vty** *n* command, where *n* is the connection number displayed in the **show ip ssh** command output, may be used instead of the **disconnect ssh** command.

When the EXEC connection ends, whether normally or abnormally, the SSH connection also ends.

Examples

The following example terminates SSH connection number 1:

```
disconnect ssh 1
```

Related Commands

Command	Description
clear line vty	Returns a terminal line to idle state using the privileged EXEC command.

dn

To associate the identity of a router with the distinguished name (DN) in the certificate of the router, use the **dn** command in crypto identity configuration mode. To remove this command from your configuration, use the **no** form of this command.

dn *name=string* [, *name=string*]

no dn *name=string* [, *name=string*]

Syntax Description

name=string	Identity used to restrict access to peers with specific certificates. Optionally, you can associate more than one identity.

Command Default

If this command is not enabled, the router can communicate with any encrypted interface that is not restricted on its IP address.

Command Modes

Crypto identity configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

Use the **dn** command to associate the identity of the router, which is defined in the **crypto identity** command, with the DN that the peer used to authenticate itself.

Note The *name* defined in the **crypto identity** command must match the *string* defined in the **dn** command. That is, the identity of the peer must be the same as the identity in the exchanged certificate.

This command allows you set restrictions in the router configuration that prevent those peers with specific certificates, especially certificates with particular DNs, from having access to selected encrypted interfaces.

An encrypting peer matches this list if it contains the attributes listed in any one line defined within the *name=string*.

Examples

The following example shows how to configure an IPsec crypto map that can be used only by peers that have been authenticated by the DN and if the certificate belongs to “green”:

```
crypto map map-to-green 10 ipsec-isakmp
 set peer 172.21.114.196
 set transform-set my-transformset
 match address 124
 identity to-green
!
crypto identity to-green
 dn ou=green
```

Related Commands

Command	Description
crypto identity	Configures the identity of the router with a given list of DNs in the certificate of the router.
fqdn	Associates the identity of the router with the hostname that the peer used to authenticate itself.

dn (IKEv2)

To enable and derive an IKEv2 name mangler from identity of type distinguished name (DN), use the **dn** command in IKEv2 name mangler configuration mode. To remove the name derived from DN, use the **no** form of this command.

dn {**common-name** | **country** | **domain** | **locality** | **organization** | **organization-unit** | **state**}

no dn

Syntax Description

common-name	Derives the name mangler from the common name portion in the DN.
country	Derives the name mangler from the country portion in the DN.
domain	Derives the name mangler from the domain portion in the DN.
locality	Derives the name mangler from the locality portion in the DN.
organization	Derives the name mangler from the organization portion in the DN.
organization-unit	Derives the name mangler from the organization-unit portion in the DN.
state	Derives the name mangler from the state portion in the DN.

Command Default

No default behavior or values.

Command Modes

IKEv2 name mangler configuration (config-ikev2-name-mangler)

Command History

Release	Modification
15.1(3)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to derive the name mangler from any field in the remote identity of type DN.

Examples

The following example shows how to derive a name for the name mangler from the country field of the DN:

```
Router(config)# crypto ikev2 name-mangler mangler2
Router(config-ikev2-name-mangler)# dn country
```

Related Commands

Command	Description
crypto ikev2 name mangler	Defines a name mangler.

dnis (AAA preauthentication)

To preauthenticate calls on the basis of the Dialed Number Identification Service (DNIS) number, use the **dnis** command in AAA preauthentication configuration mode. To remove the **dnis** command from your configuration, use the **no** form of this command.

dnis [**if-avail** | **required**] [**accept-stop**] [**password** *string*]

no dnis [**if-avail** | **required**] [**accept-stop**] [**password** *string*]

Syntax Description

if-avail	(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.
required	(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.
accept-stop	(Optional) Prevents subsequent preauthentication elements from being tried once preauthentication has succeeded for a call element.
password *string*	(Optional) Password to use in the Access-Request packet. The default is cisco.

Defaults

The **if-avail** and **required** keywords are mutually exclusive. If the **if-avail** keyword is not configured, the preauthentication setting defaults to **required**.

The default password string is cisco.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

You may configure more than one of the AAA preauthentication commands (**clid**, **ctype**, **dnis**) to set conditions for preauthentication. The sequence of the command configuration decides the sequence of the preauthentication conditions. For example, if you configure **dnis**, then **clid**, then **ctype**, then this is the order of the conditions considered in the preauthentication process.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

Examples

The following example enables DNIS preauthentication using a RADIUS server and the password Ascend-DNIS:

```
aaa preauth
 group radius
 dnis password Ascend-DNIS
```

The following example specifies that incoming calls be preauthenticated on the basis of the DNIS number:

```
aaa preauth
 group radius
 dnis required
```

Related Commands

Command	Description
aaa preauth	Enters AAA preauthentication mode.
clid	Preauthenticates calls on the basis of the CLID number.
ctype	Preauthenticates calls on the basis of the call type.
dnis bypass (AAA preauthentication configuration)	Specifies a group of DNIS numbers that will be bypassed for preauthentication.
group (authentication)	Selects the security server to use for AAA preauthentication.
isdn guard-timer	Sets a guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request.

dnis (RADIUS)

To preauthenticate calls on the basis of the DNIS (Dialed Number Identification Service) number, use the **dnis** command in AAA preauthentication configuration mode. To remove the **dnis** command from your configuration, use the **no** form of this command.

dnis [**if-avail** | **required**] [**accept-stop**] [**password** *password*]

no dnis [**if-avail** | **required**] [**accept-stop**] [**password** *password*]

Syntax Description

if-avail	(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.
required	(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.
accept-stop	(Optional) Prevents subsequent preauthentication elements such as **clid** or **ctype** from being tried once preauthentication has succeeded for a call element.
password *password*	(Optional) Defines the password for the preauthentication element.

Defaults

The **if-avail** and **required** keywords are mutually exclusive. If the **if-avail** keyword is not configured, the preauthentication setting defaults to **required**.

The default password string is cisco.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You may configure more than one of the authentication, authorization, and accounting (AAA) preauthentication commands (**clid**, **ctype**, **dnis**) to set conditions for preauthentication. The sequence of the command configuration decides the sequence of the preauthentication conditions. For example, if you configure **dnis**, then **clid**, then **ctype**, in this order, then this is the order of the conditions considered in the preauthentication process.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

Examples

The following example specifies that incoming calls be preauthenticated on the basis of the DNIS number:

```
aaa preauth
 group radius
 dnis required
```

Related Commands

Command	Description
clid	Preauthenticates calls on the basis of the CLID number.
ctype	Preauthenticates calls on the basis of the call type.
dnis bypass (AAA preauthentication configuration)	Specifies a group of DNIS numbers that will be bypassed for preauthentication.
group (RADIUS)	Specifies the AAA RADIUS server group to use for preauthentication.

dnis bypass (AAA preauthentication configuration)

To specify a group of DNIS (Dialed Number Identification Service) numbers that will be bypassed for preauthentication, use the **dnis bypass** command in AAA preauthentication configuration mode. To remove the **dnis bypass** command from your configuration, use the **no** form of this command.

dnis bypass {*dnis-group-name*}

no dnis bypass {*dnis-group-name*}

Syntax Description

dnis-group-name	Name of the defined DNIS group.

Defaults

No DNIS numbers are bypassed for preauthentication.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Before using this command, you must first create a DNIS group with the **dialer dnis group** command.

Examples

The following example specifies that preauthentication be performed on all DNIS numbers except for two DNIS numbers (12345 and 12346), which have been defined in the DNIS group called hawaii:

```
aaa preauth
 group radius
 dnis required
 dnis bypass hawaii

dialer dnis group hawaii
 number 12345
 number 12346
```

Related Commands

Command	Description
dialer dnis group	Creates a DNIS group.
dnis (RADIUS)	Preauthenticates calls on the basis of the DNIS number.

dns

To specify the primary and secondary Domain Name Service (DNS) servers, use the **dns** command in ISAKMP group configuration mode or IKEv2 authorization policy configuration mode. To remove this command from your configuration, use the **no** form of this command.

dns *primary-server* [*secondary-server*]

no dns *primary-server* [*secondary-server*]

Syntax Description

primary-server	Name of the primary DNS server.
secondary-server	(Optional) Name of the secondary DNS server.

Defaults

A DNS server is not specified.

Command Modes

ISAKMP group configuration (config-isakmp-group)
IKEv2 authorization policy configuration (config-ikev2-author-policy)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use the **dns** command to specify the primary and secondary DNS servers for the group.

You must enable the following commands before enabling the **dns** command:

- **crypto isakmp client configuration group**—Specifies the group policy information that has to be defined or changed.
- **crypto ikev2 authorization policy**—Specifies the local group policy authorization parameters.

Examples

The following example shows how to define a primary and secondary DNS server for the default group name:

```
crypto isakmp client configuration group default
 key cisco
 dns 10.2.2.2 10.3.2.3
 pool dog
 acl 199
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto ikev2 authorization policy	Specifies an IKEv2 authorization policy.
crypto isakmp client configuration group	Specifies the policy profile of the group that will be defined.
domain (isakmp-group)	Specifies the DNS domain to which a group belongs.

dnsix-dmdp retries

To set the retransmit count used by the Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) Message Delivery Protocol (DMDP), use the **dnsix-dmdp retries** command in global configuration mode. To restore the default number of retries, use the **no** form of this command.

dnsix-dmdp retries *count*

no dnsix-dmdp retries *count*

Syntax Description

count	Number of times DMDP will retransmit a message. It can be an integer from 0 to 200. The default is 4 retries, or until acknowledged.

Defaults

Retransmits messages up to 4 times, or until acknowledged.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example sets the number of times DMDP will attempt to retransmit a message to 150:

```
dnsix-dmdp retries 150
```

Related Commands

Command	Description
dnsix-nat authorized-redirection	Specifies the address of a collection center that is authorized to change the primary and secondary addresses of the host to receive audit messages.
dnsix-nat primary	Specifies the IP address of the host to which DNSIX audit messages are sent.
dnsix-nat secondary	Specifies an alternate IP address for the host to which DNSIX audit messages are sent.
dnsix-nat source	Starts the audit-writing module and defines audit trail source address.
dnsix-nat transmit-count	Causes the audit-writing module to collect multiple audit messages in the buffer before sending the messages to a collection center.

dnsix-nat authorized-redirection

To specify the address of a collection center that is authorized to change the primary and secondary addresses of the host to receive audit messages, use the **dnsix-nat authorized-redirection** command in global configuration mode. To delete an address, use the **no** form of this command.

dnsix-nat authorized-redirection *ip-address*

no dnsix-nat authorized-redirection *ip-address*

Syntax Description

ip-address	IP address of the host from which redirection requests are permitted.

Defaults

An empty list of addresses.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use multiple **dnsix-nat authorized-redirection** commands to specify a set of hosts that are authorized to change the destination for audit messages. Redirection requests are checked against the configured list, and if the address is not authorized the request is rejected and an audit message is generated. If no address is specified, no redirection messages are accepted.

Examples

The following example specifies that the address of the collection center that is authorized to change the primary and secondary addresses is 192.168.1.1:

```
dnsix-nat authorization-redirection 192.168.1.1
```

dnsix-nat primary

To specify the IP address of the host to which Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) audit messages are sent, use the **dnsix-nat primary** command in global configuration mode. To delete an entry, use the **no** form of this command.

dnsix-nat primary *ip-address*

no dnsix-nat primary *ip-address*

Syntax Description

ip-address	IP address for the primary collection center.

Defaults

Messages are not sent.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

An IP address must be configured before audit messages can be sent.

Examples

The following example configures an IP address as the address of the host to which DNSIX audit messages are sent:

```
dnsix-nat primary 172.16.1.1
```

dnsix-nat secondary

To specify an alternate IP address for the host to which Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) audit messages are sent, use the **dnsix-nat secondary** command in global configuration mode. To delete an entry, use the **no** form of this command.

dnsix-nat secondary *ip-address*

no dnsix-nat secondary *ip-address*

Syntax Description

ip-address	IP address for the secondary collection center.

Defaults

No alternate IP address is known.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the primary collection center is unreachable, audit messages are sent to the secondary collection center instead.

Examples

The following example configures an IP address as the address of an alternate host to which DNSIX audit messages are sent:

```
dnsix-nat secondary 192.168.1.1
```

dnsix-nat source

To start the audit-writing module and to define the audit trail source address, use the **dnsix-nat source** command in global configuration mode. To disable the Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) audit trail writing module, use the **no** form of this command.

dnsix-nat source *ip-address*

no dnsix-nat source *ip-address*

Syntax Description

ip-address	Source IP address for DNSIX audit messages.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You must issue the **dnsix-nat source** command before any of the other **dnsix-nat** commands. The configured IP address is used as the source IP address for DMDP protocol packets sent to any of the collection centers.

Examples

The following example enables the audit trail writing module, and specifies that the source IP address for any generated audit messages should be the same as the primary IP address of Ethernet interface 0:

```
dnsix-nat source 192.168.2.5
interface ethernet 0
 ip address 192.168.2.5 255.255.255.0
```

dnsix-nat transmit-count

To have the audit writing module collect multiple audit messages in the buffer before sending the messages to a collection center, use the **dnsix-nat transmit-count** command in global configuration mode. To revert to the default audit message count, use the **no** form of this command.

dnsix-nat transmit-count *count*

no dnsix-nat transmit-count *count*

Syntax Description

count	Number of audit messages to buffer before transmitting to the server. It can be an integer from 1 to 200.

Defaults

One message is sent at a time.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

An audit message is sent as soon as the message is generated by the IP packet-processing code. The audit writing module can, instead, buffer up to several audit messages before transmitting to a collection center.

Examples

The following example configures the system to buffer five audit messages before transmitting them to a collection center:

```
dnsix-nat transmit-count 5
```

dns-timeout

To specify the Domain Name System (DNS) idle timeout (the length of time for which a DNS lookup session will continue to be managed while there is no activity), use the **dns-timeout** command in parameter-map type inspect configuration mode. To disable the timeout, use the **no** form of this command.

dns-timeout *seconds*

no dns-timeout *seconds*

Syntax Description

seconds	Length of time, in seconds, for which a DNS name lookup session will still be managed while there is no activity. The default is 5.

Command Default

The DNS idle timeout is disabled.

Command Modes

Parameter-map type inspect configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use the **dns-timeout** subcommand when you are creating an inspect type parameter map. You can enter the **dns-timeout** subcommand after you enter the **parameter-map type inspect** command.

Use the **dns-timeout** command if you have DNS inspection configured and want to control the timeout of DNS sessions.

If DNS inspection is not configured, but you enter the **dns-timeout** command, the command does not take effect (that is, it is not applied to a DNS session).

For more detailed information about creating a parameter map, see the **parameter-map type inspect** command.

Examples

The following example specifies that if there is no activity, a DNS lookup session will continue to be managed for 25 seconds:

```
parameter-map type inspect insp-params
 dns-timeout 25
```

Related Commands

Command	Description
ip inspect dns-timeout	Specifies the DNS idle timeout (the length of time during which a DNS name lookup session will still be managed while there is no activity).
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

domain (AAA)

To configure username domain options for the RADIUS application, use the **domain** command in dynamic authorization local server configuration mode. To disable the username domain options configured, use the **no** form of this command.

domain {**delimiter** *character* | **stripping** [**right-to-left**]}

no domain {**delimiter** *character* | **stripping** [**right-to-left**]}

Syntax Description

delimiter *character*	Specifies the domain delimiter. One of the following options can be specified: **@**, **/**, **$**, **%**, ****, **#** or **-**
stripping	Compares the incoming username with the names oriented to the left of the @ domain delimiter.
right-to-left	Terminates the string at the first delimiter going from right to left.

Command Default

No username domain options are configured.

Command Modes

Dynamic authorization local server configuration (config-locsvr-da-radius)

Command History

Release	Modification
12.2(31)SB14	This command was introduced.
12.2(33)SRC5	This command was integrated into Cisco IOS Release 12.2(33)SRC5.
Cisco IOS XE Release 2.3	This command was modified. This command was implemented on ASR 1000 series routers.
15.1(2)T	This command was integrated into Cisco IOS Release 15.1(2)T. This command was also modified. The **right-to-left** keyword was added.

Usage Guidelines

If domain stripping is not configured, the full username provided in the authentication, authorization, and accounting (AAA) packet of disconnect (POD) messages is compared with the online subscribers. Configuring domain stripping allows you to send disconnect messages with only the username present before the @ domain delimiter. The network access server (NAS) compares and matches this username with any online subscriber with a potential domain.

For instance, when domain stripping is configured and you send a POD message with the username "test," a comparison between the POD message and online subscribers takes place, and subscribers with the username "test@cisco.com" or "test" match the specified username "test."

Examples

The following configuration example is used to match a username from right to left. If the username is user1@cisco.com@test.com, then the username to be matched by the POD message is user1@cisco.com.

```
Router# configure terminal
```

```
Router(config)# aaa server radius dynamic-author
Router(config-locsvr-da-radius)# domain stripping right-to-left
Router(config-locsvr-da-radius)# domain delimiter @
Router(config-locsvr-da-radius)# end
```

The following configuration example is used to match a username from left to right. If the username is user1@cisco.com@test.com, then the username to be matched by the POD message is user1.

```
Router# configure terminal
Router(config)# aaa server radius dynamic-author
Router(config-locsvr-da-radius)# domain stripping
Router(config-locsvr-da-radius)# domain delimiter @
Router(config-locsvr-da-radius)# end
```

Related Commands

Command	Description
aaa server radius dynamic-author	Configures a device as a AAA server to facilitate interaction with an external policy server.

domain (isakmp-group)

To specify the Domain Name Service (DNS) domain to which a group belongs, use the **domain** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove this command from your configuration, use the **no** form of this command.

domain *name*

no domain *name*

Syntax Description

name	Name of the DNS domain.

Defaults

A DNS domain is not specified.

Command Modes

ISAKMP group configuration (config-isakmp-group)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **domain** command to specify group domain membership.

You must enable the **crypto isakmp configuration group** command, which specifies group policy information that has to be defined or changed, before enabling the **domain** command.

Examples

The following example shows that members of the group “cisco” also belong to the domain “cisco.com”:

```
crypto isakmp client configuration group cisco
  key cisco
  dns 10.2.2.2 10.3.2.3
  pool dog
  acl 199
  domain cisco.com
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto isakmp client configuration group	Specifies the DNS domain to which a group belongs.
crypto isakmp keepalive	Specifies the primary and secondary DNS servers.

dot1x control-direction

Note Effective with Cisco IOS Release 12.2(33)SXI, the **dot1x control-direction** command is replaced by the **authentication control-direction** command. See the **authentication control-direction** command for more information.

To change an IEEE 802.1X controlled port to unidirectional or bidirectional, use the **dot1x control-direction** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

dot1x control-direction {**both** | **in**}

no dot1x control-direction

Syntax Description

both	Enables bidirectional control on the port.
in	Enables unidirectional control on the port.

Command Default

The port is set to bidirectional mode.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(25)SEC	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Switches (ISRs) only.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was replaced by the **authentication control-direction** command.

Usage Guidelines

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. 802.1x controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. 802.1x authenticates each user device that is connected to a switch port and assigns the port to a VLAN before making available any services that are offered by the switch or the LAN. Until the device is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the device is connected. After authentication is successful, normal traffic can pass through the port.

Unidirectional State

When you configure a port as unidirectional with the **dot1x control-direction in** interface configuration command, the port changes to the spanning-tree forwarding state.

When Unidirectional Controlled Port is enabled, the connected host is in the sleeping mode or power-down state. The host does not exchange traffic with other devices in the network. The host connected to the unidirectional port cannot send traffic to the network, the host can only receive traffic from other devices in the network.

Bidirectional State

When you configure a port as bidirectional with the **dot1x control-direction both** interface configuration command, the port is access-controlled in both directions. In this state, the switch port receives or sends only EAPOL packets; all other packets are dropped.

Using the **both** keyword or using the **no** form of this command changes the port to its bidirectional default setting.

Catalyst 6500 Series Switch

Setting the port as bidirectional enables 802.1X authentication with wake-on-LAN (WoL).

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time; that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows how to enable unidirectional control:

```
Switch(config-if)# dot1x control-direction in
```

The following examples show how to enable bidirectional control:

```
Switch(config-if)# dot1x control-direction both
```

or

```
Switch(config-if)# no dot1x control-direction
```

You can verify your settings by entering the **show dot1x all** privileged EXEC command. The **show dot1x all** command output is the same for all devices except for the port names and the state of the port. If a host is attached to the port but is not yet authenticated, a display similar to the following appears:

```
Supplicant MAC 0002.b39a.9275
AuthSM State = CONNECTING
BendSM State = IDLE
PortStatus = UNAUTHORIZED
```

If you enter the **dot1x control-direction in** command to enable unidirectional control, the following appears in the **show dot1x all** command output:

```
ControlDirection = In
```

If you enter the **dot1x control-direction in** command and the port cannot support this mode because of a configuration conflict, the following appears in the **show dot1x all** command output:

```
ControlDirection = In (Disabled due to port settings):
```

The following example shows how to reset the global 802.1X parameters:

```
Switch(config)# dot1x default
```

Catalyst 6500 Series Switch

The following example shows how to enable 802.1X authentication with WoL and set the port as bidirectional:

```
Switch(config)# interface gigabitethernet 5/1
Switch(config-if)# dot1x control-direction both
```

802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)X

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
 dot1x reauthentication
 dot1x control-direction in
```

Related Commands

Command	Description
show dot1x	Displays details for an identity profile.

dot1x credentials

To specify which 802.1X credential profile to use when configuring a supplicant (client) or to apply a credentials structure to an interface and to enter dot1x credentials configuration mode, use the **dot1x credentials** command in global configuration or interface configuration mode. To remove the credential profile, use the **no** form of this command.

dot1x credentials *name*

no dot1x credentials

Syntax Description

name	Name of the credentials profile.

Command Default

A credentials profile is not specified.

Command Modes

Global configuration
Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

An 802.1X credential structure is necessary when configuring a supplicant. This credentials structure may contain a username, password, and description.

Examples

The following example shows which credentials profile should be used when configuring a supplicant:

```
dot1x credentials basic-user
 username router
 password secret
 description This credentials profile should be used for most configured ports
```

The credentials structure can be applied to an interface, along with the **dot1x pae supplicant** command and keyword, to enable supplicant functionality on that interface.

```
interface fastethernet 0/1
 dot1x credentials basic-user
 dot1x pae supplicant
```

Related Commands

Command	Description
anonymous-id (dot1x credential)	Specifies the anonymous identity that is associated with a credentials profile.
description (dot1x credential)	Specifies the description for an 802.1X credentials profile.

Command	Description
password (dot1x credential)	Specifies the password for an 802.1X credentials profile.
username (dot1x credential)	Specifies the username for an 802.1X credentials profile.

dot1x critical (global configuration)

To configure the IEEE 802.1X critical authentication parameters, use the **dot1x critical** command in global configuration mode.

dot1x critical {**eapol** | **recovery delay** *milliseconds*}

Syntax Description

eapol	Specifies that the switch sends an EAPOL-Success message when the switch successfully authenticates the critical port.
recovery delay *milliseconds*	Specifies the recovery delay period that the switch waits to reinitialize a critical port when an unavailable RADIUS server becomes available; valid values are from 1 to 10000, in milliseconds.

Command Default

The default settings are as follows:

- **eapol**—Disabled
- *milliseconds*—1000 milliseconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SXI	The **recovery delay** keyword was replaced by the **authentication critical recovery delay** command.

Examples

This example shows how to specify that the switch sends an EAPOL-Success message when the switch successfully authenticates the critical port:

```
Switch(config)# dot1x critical eapol
```

This example shows how to set the recovery delay period that the switch waits to reinitialize a critical port when an unavailable RADIUS server becomes available:

```
Switch(config)# dot1x critical recovery delay 1500
```

Related Commands

Command	Description
dot1x critical (interface configuration)	Enables 802.1X critical authentication on an interface.

dot1x critical (interface configuration)

To enable 802.1X critical authentication, and optionally, 802.1X critical authentication recovery and authentication, on an interface, use the **dot1x critical** command in interface configuration mode. To disable 802.1X critical authentication, and optionally, 802.1X critical authentication recovery and authentication, use the **no** form of this command.

dot1x critical [**recovery action reinitialize**]

no dot1x critical [**recovery action reinitialize**]

Syntax Description

recovery action reinitialize	(Optional) Enables 802.1X critical authentication recovery and specifies that the port is authenticated when an authentication server is available.

Command Default

The 802.1X critical authentication is enabled on an interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Examples

This example shows how to enable 802.1X critical authentication on an interface:

```
Router(config-if)# dot1x critical
```

This example shows how to enable 802.1X critical authentication recovery and authenticate the port when an authentication server is available:

```
Router(config-if)# dot1x critical recovery action reinitialize
```

This example shows how to disable 802.1X critical authentication on an interface:

```
Router(config-if)# no dot1x critical
```

Related Commands

Command	Description
dot1x critical (global configuration)	Configures the 802.1X critical authentication parameters.

dot1x default

To reset the global 802.1X authentication parameters to their default values as specified in the latest IEEE 802.1X standard, use the **dot1x default** command in global configuration or interface configuration mode.

dot1x default

Syntax Description

This command has no arguments or keywords.

Defaults

The default values are as follows:

- The per-interface 802.1X protocol enable state is disabled (force-authorized).
- The number of seconds between reauthentication attempts is 3600 seconds.
- The quiet period is 60 seconds.
- The retransmission time is 30 seconds.
- The maximum retransmission number is 2 times.
- The multiple host support is disabled.
- The client timeout period is 30 seconds.
- The authentication server timeout period is 30 seconds.

Command Modes

Global configuration (config)
Interface configuration (config-if)

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(14)SX	This command was implemented on the Supervisor Engine 720 in Cisco IOS Release 12.2(14)SX.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 in Cisco IOS Release 12.2(17d)SXB.
12.4(6)T	Interface configuration was added as a configuration mode for this command.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. 802.1x controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. 802.1x authenticates each user device that is connected to a switch port and assigns the port to a VLAN before making available any services that are offered by the switch or the LAN. Until the device is authenticated, 802.1x access control allows only Extensible Authentication Protocol (EAP) over LAN (EAPOL) traffic through the port to which the device is connected. After authentication is successful, normal traffic can pass through the port.

Use the **show dot1x** command to verify your current 802.1X settings.

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time; that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows how to reset the global 802.1X parameters:

```
Router(config)# dot1x default
```

The following example show how to reset the global 802.1X parameters on FastEthernet interface 0:

```
Router(config)# interface FastEthernet0
Router(config-if)# dot1x default
```

Related Commands

Command	Description
dot1x critical (global configuration)	Configures the 802.1X critical authentication parameters.
dot1x critical (interface configuration)	Enables 802.1X critical authentication on an interface.
dot1x max-req	Sets the maximum number of times that the device sends an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.
dot1x re-authentication (EtherSwitch)	Enables periodic reauthentication of the client for the Ethernet switch network module.
dot1x timeout (EtherSwitch)	Sets retry timeouts for the Ethernet switch network module.
show dot1x	Displays 802.1X information.
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

dot1x guest-vlan

To specify an active VLAN as an IEEE 802.1x guest VLAN, use the **dot1x guest-vlan** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

dot1x guest-vlan *vlan-id*

no dot1x guest-vlan

Syntax Description

vlan-id	Specify an active VLAN as an IEEE 802.1x guest VLAN. The range is 1 to 4094.

Command Default

No guest VLAN is configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)EA1	This command was introduced.
12.2(25)SE	This command was modified to change the default guest VLAN behavior.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can configure a guest VLAN on a static-access port.

For each IEEE 802.1x port, you can configure a guest VLAN to provide limited services to clients (a device or workstation connected to the switch) not running IEEE 802.1x authentication. These users might be upgrading their systems for IEEE 802.1x authentication, and some hosts, such as Windows 98 systems, might not be IEEE 802.1x capable.

When you enable a guest VLAN on an IEEE 802.1x port, the software assigns clients to a guest VLAN when it does not receive a response to its Extensible Authentication Protocol over LAN (EAPOL) request/identity frame or when EAPOL packets are not sent by the client.

With Cisco IOS Release 12.4(11)T and later, the switch port maintains the EAPOL packet history. If another EAPOL packet is detected on the interface during the lifetime of the link, the guest VLAN feature is disabled. If the port is already in the guest VLAN state, the port returns to the unauthorized state, and authentication restarts. The EAPOL history is reset upon loss of link.

Any number of non-IEEE 802.1x-capable clients are allowed access when the switch port is moved to the guest VLAN. If an IEEE 802.1x-capable client joins the same port on which the guest VLAN is configured, the port is put into the unauthorized state in the RADIUS-configured or user-configured access VLAN, and authentication is restarted.

Guest VLANs are supported on IEEE 802.1x switch ports in single-host or multi-host mode.

You can configure any active VLAN except a Remote Switched Port Analyzer (RSPAN) VLAN or a voice VLAN as an IEEE 802.1x guest VLAN. The guest VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.

After you configure a guest VLAN for an IEEE 802.1x port to which a DHCP client is connected, you might need to get a host IP address from a DHCP server. You can change the settings for restarting the IEEE 802.1x authentication process on the switch before the DHCP process on the client times out and tries to get a host IP address from the DHCP server. You should decrease the settings for the IEEE 802.1x authentication process using the **dot1x max-reauth-req** and **dot1x timeout tx-period** interface configuration commands. The amount of decrease depends on the connected IEEE 802.1x client type.

Examples

This example shows how to specify VLAN 5 as an IEEE 802.1x guest VLAN:

```
Switch(config-if)# dot1x guest-vlan 5
```

This example shows how to set 3 as the quiet time on the switch, to set 15 as the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending the request, and to enable VLAN 2 as an IEEE 802.1x guest VLAN when an IEEE 802.1x port is connected to a DHCP client:

```
Switch(config-if)# dot1x timeout max-reauth-req 3
Switch(config-if)# dot1x timeout tx-period 15
Switch(config-if)# dot1x guest-vlan 2
```

You can display the IEEE 802.1x administrative and operational status for the device or for the specified interface by entering the **show dot1x** [**interface** *interface-id*] privileged EXEC command.

Related Commands

Command	Description
dot1x max-reauth-req	Specifies the number of times that the switch retransmits an EAP-request/identity frame to the client before restarting the authentication process.
dot1x timeout	Sets authentication retry timeouts.
show dot1x	Displays details for an identity profile.

dot1x guest-vlan supplicant

To allow the 802.1x-capable supplicants to enter the guest VLAN, use the **dot1x guest-vlan supplicant** command in global configuration mode. To prevent the 802.1x-capable supplicants from entering the guest VLAN, use the **no** form of this command.

dot1x guest-vlan supplicant

no dot1x guest-vlan supplicant

Syntax Description

This command has no arguments or keywords.

Command Default

The 802.1x-capable supplicants are prevented from entering the guest VLAN.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Examples

This example shows how to allow the 802.1x-capable supplicants to enter the guest VLAN:

```
Router(config)# dot1x guest-vlan supplicant
```

This example shows how to prevent the 802.1x-capable supplicants from entering the guest VLAN:

```
Router(config)# no dot1x guest-vlan supplicant
```

Related Commands

Command	Description
dot1x critical (global configuration)	Configures the 802.1X critical authentication parameters.
dot1x critical (interface configuration)	Enables 802.1X critical authentication on an interface.

dot1x host-mode

Note Effective with Cisco IOS Release 12.2(33)SXI, the **dot1x host-mode** command is replaced by the **authentication host-mode** command. See the **authentication host-mode** command for more information.

To allow hosts on an IEEE 802.1X-authorized port, use the **dot1x host-mode** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

dot1x host-mode {**multi-auth** | **multi-host** | **single-host**}

no dot1x host-mode {**multi-auth** | **multi-host** | **single-host**}

Syntax Description

multi-auth	Specifies that all clients are authenticated individually on the port. The multi-auth mode is not supported on switch ports and is the default mode for switch ports.
multi-host	Ensures that the first client and all subsequent clients are allowed access to the port if the first client is successfully authenticated.
single-host	Ensures that only the first client is authenticated. All other clients are ignored and may cause a violation. The single-host mode is the default mode for switch ports.

Command Default

Hosts are not allowed on an 802.1X-authorized port.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)EA1	This command was introduced for switches. It replaced the **dot1x multiple-hosts** command.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Switches (ISRs) only.
12.2(33)SXI	This command was replaced by the **authentication host-mode** command.

Usage Guidelines

Before you use this command, use the **dot1x port-control auto** command to enables IEEE 802.1X port-based authentication, and cause the port to begin in the unauthorized state.

The **multi-auth** mode authenticates each new client separately.

In **multi-host** mode, only one of the attached hosts has to be successfully authorized for all hosts to be granted network access (the **multi-host** mode authenticates one client, but after the client is authenticated, traffic is allowed from all other MAC addresses.). If the port becomes unauthorized (reauthentication fails or an Extensible Authentication Protocol over LAN [EAPOL] logoff message is received), all attached clients are denied access to the network.

The **single-host** mode allows only one client per port; that is, one MAC address is authenticated, and all others are blocked.

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time; that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows how to enable IEEE 802.1X globally, to enable IEEE 802.1x on a port, and to enable multiple-hosts mode:

```
Switch(config)# dot1x system-auth-control
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host:
```

802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)XC

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
 dot1x reauthentication
```

Related Commands

Command	Description
dot1x port-control	Enables 802.1X port-based authentication.
show dot1x	Displays details for an identity profile.

dot1x initialize

Note Effective with Cisco IOS Release 12.2(33)SXI, the **dot1x initialize** command is replaced by the **clear authentication session** command. See the **clear authentication session** command for more information.

To initialize 802.1X clients on all 802.1X-enabled interfaces, use the **dot1x initialize** command in privileged EXEC mode. This command does not have a **no** form.

dot1x initialize [**interface** *interface-name*]

Syntax Description

interface *interface-name*	(Optional) Specifies an interface to be initialized. If this keyword is not entered, all interfaces are initialized.

Defaults

State machines are not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)EA1	This command was introduced.
12.3(2)XA	This command was integrated into Cisco IOS Release 12.3(2)XA.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

Use this command to initialize the 802.1X state machines and to set up a fresh environment for authentication. After you enter this command, the port status becomes unauthorized.

Examples

The following example shows how to manually initialize a port:

```
Router# dot1x initialize interface gigabitethernet2/0/2
```

You can verify the unauthorized port status by entering the **show dot1x** [**interface** *interface-name*] command.

Related Commands

Command	Description
show dot1x	Displays details for an identity profile.

dot1x mac-auth-bypass

To enable a switch to authorize clients based on the client MAC address, use the **dot1x mac-auth-bypass** command in interface configuration mode. To disable MAC authentication bypass, use the **no** form of this command.

dot1x mac-auth-bypass [**eap**]

no dot1x mac-auth-bypass

Syntax Description

eap	(Optional) Configures the switch to use Extensible Authentication Protocol (EAP) for authorization.

Command Default

MAC authentication bypass is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Note To use MAC authentication bypass on a routed port, ensure that MAC address learning is enabled on the port.

When the MAC authentication bypass feature is enabled on an 802.1X port, the switch uses the MAC address as the client identity. The authentication server has a database of client MAC addresses that are allowed network access. If authorization fails, the switch assigns the port to the guest VLAN if a VLAN is configured.

Examples

This example shows how to enable MAC authentication bypass:

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x mac-auth-bypass
```

This example shows how to configure the switch to use EAP for authorization:

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x mac-auth-bypass eap
```

This example shows how to disable MAC authentication bypass:

```
Router(config)# interface fastethernet 5/1
Router(config-if)# no dot1x mac-auth-bypass
```

Related Commands

Command	Description
dot1x critical (global configuration)	Configures the 802.1X critical authentication parameters.
dot1x critical (interface configuration)	Enables 802.1X critical authentication on an interface.

dot1x max-reauth-req

To set the maximum number of times the authenticator sends an Extensible Authentication Protocol (EAP) request/identity frame (assuming that no response is received) to the client , use the **dot1x max-reauth-req** command in interface configuration mode. To set the maximum number of times to the default setting of 2, use the **no** form of this command.

dot1x max-reauth-req *number*

no dot1x max-reauth-req

Syntax Description

number	Maximum number of times. The range is 1 through 10. The default is 2.

Command Default

The command default is 2.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SE	This command was introduced.
12.2(25)SEC	The *number* argument was added.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.

Usage Guidelines

You should change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Verifying Settings

You can verify your settings by entering the **show dot1x** [**interface** *interface-id*] command.

Examples

The following example shows how to set 4 as the number of times that the authentication process is restarted before changing to the unauthorized state:

```
Router(config-if)# dot1x max-reauth-req 4
```

802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)XC

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
 dot1x reauthentication
```

Related Commands

Command	Description
dot1x max-req	Sets the maximum number of times that a device can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process .
dot1x timeout tx-period	Sets the number of seconds that the switch waits for a response to an EAP request or identity frame from the client before resending the request.
show dot1x	Displays IEEE 802.1X status for the specified port.

dot1x max-req

To set the maximum number of times that a networking device or Ethernet switch network module can send an Extensible Authentication Protocol (EAP) request/identity frame to a client (assuming that a response is not received) before restarting the authentication process, use the **dot1x max-req** command in interface configuration or global configuration mode. To set the number of times to the default setting of 2, use the **no** form of this command.

dot1x max-req *retry-number*

no dot1x max-req

Syntax Description

retry-number	Maximum number of retries. The value is from 1 through 10. The default value is 2. The value is applicable to all EAP packets except for Request ID.

Defaults

The default number of retries is 2.

Command Modes

Interface configuration (config-if)
Global configuration (config)

Command History

Release	Modification
12.1(6)EA2	This command was introduced on the Cisco Ethernet switch network module.
12.2(14)SX	This command was implemented on the Supervisor Engine 720 in Cisco IOS Release 12.2(14)SX.
12.2(15)ZJ	This command was implemented on the Cisco Ethernet switch network module on the following platforms in Cisco IOS Release 12.2(15)ZJ: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series.
12.1(11)AX	This command was integrated into Cisco IOS Release 12.1(11)AX.
12.1(14)EA1	This command was integrated into Cisco IOS Release 12.1(14)EA1 and the configuration mode was changed to interface configuration mode except on the EtherSwitch network module.
12.3(2)XA	This command was integrated into Cisco IOS Release 12.3(2)XA and implemented on the following router platforms: Cisco 806, Cisco 831, Cisco 836, Cisco 837, Cisco 1701, Cisco 1710, Cisco 1721, Cisco 1751-V, and Cisco 1760.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T and implemented on the following router platforms: Cisco 1751, Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3640, Cisco 3640A, and Cisco 3660.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 in Cisco IOS Release 12.2(17d)SXB.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.(33)SXH.

Usage Guidelines

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. 802.1x controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. 802.1x authenticates each user device that is connected to a switch port and assigns the port to a VLAN before making available any services that are offered by the switch or the LAN. Until the device is authenticated, 802.1x access control allows only Extensible Authentication Protocol (EAP) over LAN (EAPOL) traffic through the port to which the device is connected. After authentication is successful, normal traffic can pass through the port.

Note You should change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows that the maximum number of times that the networking device will send an EAP request or identity message to the client PC is 6:

```
Router(config) configure terminal
Router(config)# interface ethernet 0
Router(config-if)# dot1x max-req 6
```

The following example shows how to set the number of times that a switch sends an EAP request or identity frame to 5 before restarting the authentication process:

```
Router(config-if)# dot1x max-req 5
```

Related Commands

Command	Description
dot1x port-control	Enables manual control of the authorization state of a controlled port.
dot1x re-authentication	Globally enables periodic reauthentication of the client PCs on the 802.1X interface.
dot1x reauthentication (EtherSwitch)	Enables periodic reauthentication of the Ethernet switch network module client on the 802.1X interface.
dot1x timeout	Sets retry timeouts.
dot1x timeout (EtherSwitch)	Sets retry timeouts for the Ethernet switch network module.

Command	Description
show dot1x	Displays details for an identity profile.
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

dot1x max-start

To set the maximum number of Extensible Authentication Protocol (EAP) start frames that a supplicant sends (assuming that no response is received) to the client before concluding that the other end is 802.1X unaware, use the **dot1x max-start** command in global configuration or interface configuration mode. To remove the maximum number-of-times setting, use the **no** form of this command.

dot1x max-start *number*

no dot1x max-start

Syntax Description

number	Maximum number of times that the router sends an EAP start frame. The value is from 1 to 65535. The default is 3.

Defaults

The default maximum number setting is 3.

Command Modes

Global configuration
Interface configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.4(6)T	Global configuration mode was added for this command.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows that the maximum number of EAP over LAN- (EAPOL-) Start requests has been set to 5:

```
Router (config)# interface Ethernet1
Router (config-if)# dot1x pae supplicant
Router (config-if)# dot1x max-start 5
```

802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)XC

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
 dot1x reauthentication
```

Related Commands

Command	Description
dot1x pae	Sets the PAE type during 802.1X authentication.
interface	Configures an interface type.

dot1x multi-hosts

To allow multiple hosts (clients) on an 802.1X-authorized port in interface configuration command mode, use the **dot1x multi-hosts** command. Use the **no** form of this command to disallow multiple hosts.

dot1x multi-hosts

no dot1x multi-hosts

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

Before entering this command, ensure that the **dot1x port-control** command is set to **auto** for the specified interface.

Examples

This example shows how to allow multiple hosts:

```
Router(config-if)# dot1x multi-hosts
Router(config-if)#
```

This example shows how to disallow multiple hosts:

```
Router(config-if)# no dot1x multi-hosts
Router(config-if)#
```

Related Commands

Command	Description
dot1x port-control	Sets the port control value.
show dot1x	Displays 802.1X information.

dot1x multiple-hosts

Note This command was replaced by the **dot1x host-mode** command effective with Cisco IOS Release 12.1(14)EA1 and Release 12.4(6)T.

To allow multiple hosts (clients) on an 802.1X-authorized switch port that has the **dot1x port-control** interface configuration command set to **auto**, use the **dot1x multiple-hosts** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

dot1x multiple-hosts

no dot1x multiple-hosts

Syntax Description

This command has no arguments or keywords.

Defaults

Multiple hosts are disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.1(14)EA1	This command was replaced by the **dot1x host-mode** command in Cisco IOS Release 12.1(14)EA1.
12.4(6)T	This command was replaced by the **dot1x host-mode** command on the T-train.

Usage Guidelines

This command is supported only on switch ports.

This command enables you to attach multiple clients to a single 802.1X-enabled port. In this mode, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (reauthentication fails or an Extensible Authentication Protocol over LAN [EAPOL]-logoff message is received), all attached clients are denied access to the network.

Use the **show dot1x** (EtherSwitch) privileged EXEC command with the **interface** keyword to verify your current 802.1X multiple host settings.

Examples

The following example shows how to enable 802.1X on Fast Ethernet interface 0/1 and to allow multiple hosts:

```
Router(config)# interface fastethernet0/1
Router(config-if)# dot1x port-control auto
Router(config-if)# dot1x multiple-hosts
```

Related Commands

Command	Description
dot1x default	Enables manual control of the authorization state of the port.
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

dot1x pae

To set the Port Access Entity (PAE) type, use the **dot1x pae** command in interface configuration mode. To disable the PAE type that was set, use the **no** form of this command.

dot1x pae [**supplicant | authenticator | both**]

no dot1x pae [**supplicant | authenticator | both**]

Syntax Description

supplicant	(Optional) The interface acts only as a supplicant and will not respond to messages that are meant for an authenticator.
authenticator	(Optional) The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.
both	(Optional) The interface behaves both as a supplicant and as an authenticator and thus will respond to all dot1x messages.

Defaults

PAE type is not set.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the **dot1x system-auth-control** command has not been configured, the **supplicant** keyword will be the only keyword available for use with this command. (That is, if the **dot1x system-auth-control** command has not been configured, you cannot configure the interface as an authenticator.)

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows that the interface has been set to act as a supplicant:

```
Router (config)# interface Ethernet1
```

```
Router (config-if)# dot1x pae supplicant
```

802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)XC

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
 dot1x reauthentication
```

Related Commands

Command	Description
dot1x system-auth-control	Enables 802.1X SystemAuthControl (port-based authentication).
interface	Configures an interface type.

dot1x port-control

Note Effective with Cisco IOS Release 12.2(33)SXI, the **dot1x port-control** command is replaced by the **authentication port-control** command. See the **authentication port-control** command for more information.

To enable manual control of the authorization state of a controlled port, use the **dot1x port-control** command in interface configuration mode. To disable the port-control value, use the **no** form of this command.

dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**}

no dot1x port-control

Syntax Description

auto	Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port.
force-authorized	Disables 802.1X on the interface and causes the port to change to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The **force-authorized** keyword is the default.
force-unauthorized	Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.

Defaults

The default is force-authorized.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced for the Cisco Ethernet switch network module.
12.1(11)AX	This command was integrated into Cisco IOS Release 12.1(11)AX.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(15)ZJ	This command was implemented on the following platforms for the Cisco Ethernet switch network module: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series.
12.3(2)XA	This command was introduced on the following Cisco Switches: Cisco 806, Cisco 831, Cisco 836, Cisco 837, Cisco 1701, Cisco 1710, Cisco 1721, Cisco 1751-V, and Cisco 1760.

Release	Modification
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T. Switch support was added for the following platforms: Cisco 1751, Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3640, Cisco 3640A, and Cisco 3660.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was added for Cisco IOS Release 12.2(17d)SXB.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Switches (ISRs) only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	This command was replaced by the **authentication port-control** command.

Usage Guidelines

For Ethernet Switch Network Modules

The following guidelines apply to Ethernet switch network modules:

- The 802.1X protocol is supported on Layer 2 static-access ports.
- You can use the **auto** keyword only if the port is not configured as one of these types:
  - Trunk port—If you try to enable 802.1X on a trunk port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to trunk, the port mode is not changed.
  - EtherChannel port—Before enabling 802.1X on the port, you must first remove it from the EtherChannel. If you try to enable 802.1X on an EtherChannel or on an active port in an EtherChannel, an error appears, and 802.1X is not enabled. If you enable 802.1X on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.
  - Switch Port Analyzer (SPAN) destination port—You can enable 802.1X on a port that is a SPAN destination port; however, 802.1X is disabled until the port is removed as a SPAN destination. You can enable 802.1X on a SPAN source port.

To globally disable 802.1X on the device, you must disable it on each port. There is no global configuration command for this task.

For Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time; that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Verifying Settings

You can verify your settings by entering the **show dot1x** command and checking the Status column in the 802.1X Port Summary section of the display. An enabled status means that the port-control value is set to auto or to force-unauthorized.

Examples

The following example shows that the authentication status of the client PC will be determined by the authentication process:

```
Switch(config)# configure terminal
Switch(config)# interface ethernet 0
Switch(config-if)# dot1x port-control auto
```

802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)XC

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
 dot1x reauthentication
```

Related Commands

Command	Description
dot1x max-req	Sets the maximum number of times that a switch or Ethernet switch network module can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.
dot1x re-authentication	Globally enables periodic reauthentication of the client on the 802.1X interface.
dot1x reauthentication (EtherSwitch)	Enables periodic reauthentication of the client on the 802.1X interface.
dot1x timeout	Sets retry timeouts.
dot1x timeout (EtherSwitch)	Sets retry timeouts for the Ethernet switch network module.
show dot1x	Displays details for an identity profile.
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.

dot1x re-authenticate (EtherSwitch)

To manually initiate a reauthentication of all 802.1X-enabled ports or the specified 802.1X-enabled port on a router with an Ethernet switch network module installed, use the **dot1x re-authenticate** command in privileged EXEC mode.

dot1x re-authenticate [**interface** *interface-type interface-number*]

Syntax Description

interface *interface-type interface-number*	(Optional) Specifies the slot and port number of the interface to reauthenticate.

Defaults

There is no default setting.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

You can use this command to reauthenticate a client without waiting for the configured number of seconds between reauthentication attempts (reauthperiod) and automatic reauthentication.

Examples

The following example shows how to manually reauthenticate the device connected to Fast Ethernet interface 0/1:

```
Router# dot1x re-authenticate interface fastethernet 0/1
Starting reauthentication on FastEthernet0/1.
```

dot1x re-authenticate (privileged EXEC)

Note Effective with Cisco IOS Release 12.2(33)SXI, the **dot1x re-authenticate** command is replaced by the **clear authentication session** command. See the **clear authentication session** command for more information.

To manually initiate a reauthentication of the specified 802.1X-enabled ports, use the **dot1x re-authenticate** command in privileged EXEC mode.

dot1x re-authenticate [**interface** *interface-name interface-number*]

Syntax Description

interface *interface-name interface-number*	(Optional) Interface on which reauthentication is to be initiated.

Command Default

There is no default setting.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)AX	This command was introduced.
12.3(2)XA	This command was integrated into Cisco IOS Release12.3(2)XA.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.

Usage Guidelines

You can use this command to reauthenticate a client without having to wait for the configured number of seconds between reauthentication attempts (re-authperiod) and automatic reauthentication.

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows how to manually reauthenticate the device that is connected to a port:

```
Router# dot1x re-authenticate interface gigabitethernet2/0/1
```

802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)XC

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
 dot1x reauthentication
```

Related Commands

Command	Description
dot1x reauthentication	Globally enables periodic reauthentication of the client PCs on the 802.1X interface.
dot1x timeout	Sets retry timeouts.

dot1x reauthentication

Note Effective with Cisco IOS Release 12.2(33)SXI, the **dot1x reauthentication** command is replaced by the **authentication periodic** command. See the **authentication periodic** command for more information.

To enable periodic reauthentication of the client PCs on the 802.1X interface, use the **dot1x reauthentication** command in interface configuration mode. To disable periodic reauthentication, use the **no** form of this command.

dot1x reauthentication

no dot1x reauthentication

Syntax Description

This command has no arguments or keywords.

Defaults

Periodic reauthentication is not set.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.3(2)XA	This command was integrated into Cisco IOS Release 12.3(2)XA.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 in Cisco IOS Release 12.2(17d)SXB.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	This command was replaced by the **authentication periodic** command.

Usage Guidelines

The reauthentication period can be set using the **dot1x timeout** command.

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time; that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows that reauthentication has been enabled and the reauthentication period as been set for 1800 seconds:

```
Router(config)# configure terminal
Router(config)# interface ethernet 0
Router(config-if)# dot1x reauthentication
Router(config-if)# dot1x timeout reauth-period 1800
```

802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)X

The following example shows Layer 3 802.1X support on a switched virtual interface using a Cisco 870 ISR:

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
 dot1x reauthentication
```

Cisco 7600 Series

The following example shows how to enable periodic reauthentication of the client:

```
Router(config-if)# dot1x reauthentication
Router(config-if)#
```

The following example shows how to disable periodic reauthentication of the client:

```
Router(config-if)# no dot1x reauthentication
Router(config-if)#
```

Related Commands

Command	Description
dot1x max-req	Sets the maximum number of times that a router can send an EAP request/identity frame to a client PC (assuming that a response is not received) before concluding that the client PC does not support 802.1X.
dot1x port-control	Sets an 802.1X port control value.
dot1x timeout	Sets retry timeouts.
show dot1x	Displays 802.1X information.

dot1x re-authentication (EtherSwitch)

To enable periodic reauthentication of the client for an Ethernet switch network module, use the **dot1x re-authentication** command in global configuration mode. To disable periodic reauthentication, use the **no** form of this command.

dot1x re-authentication

no dot1x re-authentication

Syntax Description

This command has no arguments or keywords.

Defaults

Periodic reauthentication is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

You configure the amount of time between periodic reauthentication attempts by using the **dot1x timeout re-authperiod** global configuration command.

Examples

The following example shows how to disable periodic reauthentication of the client:

```
Router(config)# no dot1x re-authentication
```

The following example shows how to enable periodic reauthentication and set the number of seconds between reauthentication attempts to 4000 seconds:

```
Router(config)# dot1x re-authentication
Router(config)# dot1x timeout re-authperiod 4000
```

Related Commands

Command	Description
dot1x timeout (EtherSwitch)	Sets retry timeouts for the Ethernet switch network module.
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

dot1x supplicant interface

To configure the dot1x supplicant for a given interface, use the **dot1x supplicant interface** command in privileged EXEC mode. To disable the configuration, use the **no** form of this command.

dot1x supplicant {**start** | **stop**} *profile-name* **interface** *type number*

Syntax Description

start	Starts the supplicant for a given interface.
stop	Stops the supplicant for a given interface.
profile-name	Profile name.
type number	Interface type and number.

Command Default

The dot1x supplicant interface is not configured.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to configure the dot1x supplicant for a Gigabit Ethernet interface:

```
Router# dot1x supplicant start n1 interface GigabitEthernet 0/0/1
```

Related Commands

Command	Description
dot1x default	Resets the global 802.1X authentication parameters to their default values as specified in the latest IEEE 802.1X standard.

dot1x system-auth-control

To globally enable 802.1X SystemAuthControl (port-based authentication), use the **dot1x system-auth-control** command in global configuration mode. To disable SystemAuthControl, use the **no** form of this command.

dot1x system-auth-control

no dot1x system-auth-control

Syntax Description

This command has no arguments or keywords.

Defaults

System authentication is disabled by default. If this command is disabled, all ports behave as if they are force authorized.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.2(14)SX	This command was implemented on the Supervisor Engine 720.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. 802.1x controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. 802.1x authenticates each user device that is connected to a switch port and assigns the port to a VLAN before making available any services that are offered by the switch or the LAN. Until the device is authenticated, 802.1x access control allows only Extensible Authentication Protocol (EAP) over LAN (EAPOL) traffic through the port to which the device is connected. After authentication is successful, normal traffic can pass through the port.

The **no** form of the command removes any 802.1X-related configurations.

Catalyst 6500 Series Switch and Cisco 7600 Series

You must enable Authentication, Authorization, and Accounting (AAA) and specify the authentication method list before enabling 802.1X. A method list describes the sequence and authentication methods to be queried to authenticate a user.

Examples

The following example shows how to enable SystemAuthControl:

```
Router(config)# dot1x system-auth-control
```

Related Commands

Command	Description
aaa authentication dot1x	Specifies one or more AAA methods for use on interfaces running IEEE 802.1X.
aaa new-model	Enables the AAA access-control model.
debug dot1x	Displays 802.1X debugging information.
description	Specifies a description for an 802.1X profile.
device	Statically authorizes or rejects individual devices.
dot1x initialize	Initializes 802.1X state machines on all 802.1X-enabled interfaces.
dot1x max-req	Sets the maximum number of times that a router or Ethernet switch network module can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.
dot1x port-control	Enables manual control of the authorized state of a controlled port.
dot1x re-authenticate	Manually initiates a reauthentication of the specified 802.1X-enabled ports.
dot1x reauthentication	Globally enables periodic reauthentication of the client PCs on the 802.1X interface.
dot1x timeout	Sets retry timeouts.
identity profile	Creates an identity profile and enters identity profile configuration mode.
show dot1x	Displays details and statistics for an identity profile.
template	Specifies a virtual template from which commands may be cloned.

dot1x timeout

To configure the value for retry timeouts, use the **dot1x timeout** command in global configuration or interface configuration mode. To return to the default value for retry timeouts to, use the **no** form of this command.

All Platforms Except the Cisco 7600 Series Switch

dot1x timeout {**auth-period** *seconds* | **held-period** *seconds* | **quiet-period** *seconds* | **ratelimit-period** *seconds* | **reauth-period** {*seconds* | **server**} | **server-timeout** *seconds* | **start-period** *seconds* | **supp-timeout** *seconds* | **tx-period** *seconds*}

no dot1x timeout {**auth-period** *seconds* | **held-period** *seconds* | **quiet-period** *seconds* | **ratelimit-period** *seconds* | **reauth-period** {*seconds* | **server**} | **server-timeout** *seconds* | **start-period** *seconds* | **supp-timeout** *seconds* | **tx-period** *seconds*}

Cisco 7600 Series Switch

dot1x timeout {**reauth-period** *seconds* | **quiet-period** *seconds* | **tx-period** *seconds* | **supp-timeout** *seconds* | **server-timeout** *seconds*}

no dot1x timeout {**reauth-period** | **quiet-period** | **tx-period** | **supp-timeout** | **server-timeout**}

Syntax Description

auth-period *seconds*	Configures the time, in seconds, the supplicant (client) waits for a response from an authenticator (for packets other than Extensible Authentication Protocol over LAN [EAPOL]-Start) before timing out. • The range is from 1 to 65535. The default is 30.
held-period *seconds*	Configures the time, in seconds for which a supplicant will stay in the HELD state (that is, the length of time it will wait before trying to send the credentials again after a failed attempt). • The range is from 1 to 65535. The default is 60.
quiet-period *seconds*	Configures the time, in seconds, that the authenticator (server) remains quiet (in the HELD state) following a failed authentication exchange before trying to reauthenticate the client. • For all platforms except the Cisco 7600 series Switch, the range is from 1 to 65535. The default is 120. • For the Cisco 7600 series Switch, the range is from 0 to 65535. The default is 60.
ratelimit-period *seconds*	Throttles the EAP-START packets that are sent from misbehaving client PCs (for example, PCs that send EAP-START packets that result in the wasting of switch processing power). • The authenticator ignores EAPOL-Start packets from clients that have successfully authenticated for the rate-limit period duration. • The range is from 1 to 65535. By default, rate limiting is disabled.

reauth-period {*seconds* | **server**}	Configures the time, in seconds, after which an automatic reauthentication should be initiated. • The **server** keyword indicates that the reauthentication period value for the client should be obtained from the authentication, authorization, and accounting (AAA) server as the Session-Timeout (RADIUS Attribute 27) value. If the **server** keyword is used, the action upon reauthentication is also decided by the server and sent as the Termination-Action (RADIUS Attribute 29) value. The termination action could be either "terminate" or "reauthenticate." If the **server** keyword is not used, the termination action is always "reauthenticate." • For all platforms except the Cisco 7600 series switch, the range is from 1 to 65535. The default is 3600. • For the Cisco 7600 series switch, the range is from 1 to 4294967295. The default is 3600. See the "Usage Guidelines" section for additional information. **Note** Effective with Cisco IOS Release 12.2(33)SXI, this phrase is replaced by the **authentication timer reauthenticate** command. See the **authentication timer reauthenticate** command for more information.
server-timeout *seconds*	Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted. • For all platforms except the Cisco 7600 series switch, the range is from 1 to 65535. The default is 30. • For the Cisco 7600 series switch, the range is from 30 to 65535. The default is 30. If the server does not send a response to an 802.1X packet within the specified period, the packet is sent again.
start-period *seconds*	Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted. • The value is from 1 to 65535. The default is 30.
supp-timeout *seconds*	Sets the authenticator-to-supplicant retransmission time for all EAP messages other than EAP Request ID. • For all platforms except the Cisco 7600 series Switch, the range is from 1 to 65535. The default is 30. • For the Cisco 7600 series Switch, the range is from 30 to 65535. The default is 30.
tx-period *seconds*	Configures the number of seconds between retransmission of EAP request ID packets (assuming that no response is received) to the client. • For all platforms except the Cisco 7600 series switch, the range is from 1 to 65535. The default is 30. • For the Cisco 7600 series switch, the range is from 30 to 65535. The default is 30. • If an 802.1X packet is sent to the supplicant and the supplicant does not send a response after the retry period, the packet will be sent again.

Defaults

Periodic reauthentication and periodic rate-limiting are not done.

Command Modes

Global configuration
Interface configuration

Cisco 7600 Switch

Interface configuration

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.3(2)XA	This command was integrated into Cisco IOS Release 12.3(2)XA.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(18)SE	Ranges for the **server-timeout**, **supp-timeout**, and **tx-period** keywords were changed.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was added for Cisco IOS Release 12.2(17d)SXB.
12.3(11)T	The **auth-period**, **held-period**, and **start-period** keywords were added.
12.2(25)SEC	The range for the **tx-period** keyword was changed, and the **reauth-period** and **server-timeout** keywords were added.
12.1(11)AX	This command was introduced.
12.1(14)EA1	The **supp-timeout** and **server-timeout** keywords were added. The configuration mode for the command was changed to interface configuration mode.
12.4(6)T	The **supp-timeout** keyword was added, and this command was integrated into Cisco IOS Release 12.4(6)T.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Switches (ISRs) only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	The **reauth-period** keyword was replaced by the **authentication timer reauthenticate** command.

Usage Guidelines

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time; that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Cisco 7600 Switch

You must enable periodic reauthentication before you enter the **dot1x timeout reauth-period** command. Enter the **dot1x reauthentication** command to enable periodic reauthentication. The **dot1x timeout reauth-period** command affects the behavior of the system only if periodic reauthentication is enabled.

Examples

The following example shows that various 802.1X retransmission and timeout periods have been set:

```
Switch(config)# configure terminal
Switch(config)# interface ethernet 0
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout auth-period 2000
Switch(config-if)# dot1x timeout held-period 2400
Switch(config-if)# dot1x timeout reauth-period 1800
Switch(config-if)# dot1x timeout quiet-period 600
Switch(config-if)# dot1x timeout start-period 90
Switch(config-if)# dot1x timeout supp-timeout 300
Switch(config-if)# dot1x timeout tx-period 60
Switch(config-if)# dot1x timeout server-timeout 60
```

The following example shows how to return to the default reauthorization period:

```
Switch(config-if)# no dot1x timeout reauth-period
```

Cisco 7600 Switch

The following example shows how to set 802.1X retransmission and timeout periods on the Cisco 7600 Switch:

```
Switch(config-if)# dot1x timeout reauth-period 4000
Switch(config-if)# dot1x timeout tx-period 60
Switch(config-if)# dot1x timeout supp-timeout 25
Switch(config-if)# dot1x timeout server-timeout 25
```

802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)XC

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
 dot1x reauthentication
```

Related Commands

Command	Description
dot1x max-req	Sets the maximum number of times that a switch or Ethernet switch module can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.
dot1x port-control	Sets an 802.1X port control value.

Command	Description
dot1x re-authentication	Globally enables periodic reauthentication of the client PCs on the 802.1X interface.
show dot1x	Displays 802.1X information.

dot1x timeout (EtherSwitch)

To set the number of retry seconds between 802.1X authentication exchanges when an Ethernet switch network module is installed in the router, use the **dot1x timeout** command in global configuration mode. To return to the default setting, use the **no** form of this command.

dot1x timeout {**quiet-period** *seconds* | **re-authperiod** *seconds* | **tx-period** *seconds*}

no dot1x timeout {**quiet-period** *seconds* | **re-authperiod** *seconds* | **tx-period** *seconds*}

Syntax Description

quiet-period *seconds*	Specifies the time in seconds that the Ethernet switch network module remains in the quiet state following a failed authentication exchange with the client. The range is from 0 to 65535 seconds. The default is 60 seconds.
re-authperiod *seconds*	Specifies the number of seconds between reauthentication attempts. The range is from 1 to 4294967295. The default is 3660 seconds.
tx-period *seconds*	Time in seconds that the switch should wait for a response to an EAP-request/identity frame from the client before retransmitting the request. The range is from 1 to 65535 seconds. The default is 30 seconds.

Defaults

quiet-period: 60 seconds
re-authperiod: 3660 seconds
tx-period: 30 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

You should change the default values of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients or authentication servers.

quiet-period Keyword

During the quiet period, the Ethernet switch network module does not accept or initiate any authentication requests. If you want to provide a faster response time to the user, enter a smaller number than the default.

re-authperiod Keyword

The **re-authperiod** keyword affects the behavior of the the Ethernet switch network module only if you have enabled periodic reauthentication by using the **dot1x re-authentication** global configuration command.

Examples

The following example shows how to set the quiet time on the switch to 30 seconds:

```
Router(config)# dot1x timeout quiet-period 30
```

The following example shows how to enable periodic reauthentication and set the number of seconds between reauthentication attempts to 4000 seconds:

```
Router(config)# dot1x re-authentication
Router(config)# dot1x timeout re-authperiod 4000
```

The following example shows how to set 60 seconds as the amount of time that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request:

```
Router(config)# dot1x timeout tx-period 60
```

Related Commands

Command	Description
dot1x max-req	Sets the maximum number of times that the device sends an EAP-request/identity frame before restarting the authentication process.
dot1x re-authentication (EtherSwitch)	Enables periodic reauthentication of the client for the Ethernet switch network module.
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

dpd

To configure Dead Peer Detection (DPD), use the **dpd** command in IKEv2 profile configuration mode. To delete DPD, use the **no** form of this command.

dpd *interval retry-interval* {**on-demand** | **periodic**}

no dpd

Syntax Description

interval	Specifies the keepalive interval in seconds. The range is 10 to 3600.
retry-interval	Specifies the retry interval in seconds when there is no reply from the peer.
on-demand	Specifies the on-demand mode to send the keepalive only in the absence of any incoming data traffic, to check the liveness of the peer before sending any data.
periodic	Specifies the periodic mode to send keepalives regularly at a specified interval.

Command Default

DPD is disabled by default.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to configure DPD globally for peers matching a profile. The DPD configuration in an Internet Key Exchange Version 2 (IKEv2) profile overrides the global DPD configuration.

Examples

The following example shows how to configure the periodic mode for DPD:

```
Router(config)# crypto ikev2 profile prf1
Router(config-ikev2-profile)# dpd 1000 250 periodic
```

Related Commands

Command	Description
crypto ikev2 dpd	Defines DPD globally for all peers.
crypto ikev2 profile	Defines IKEv2 profile.

drop (type access-control)

To configure a traffic class to discard packets belonging to a specific class, use the **drop** command in policy-map class configuration mode. To disable the packet discarding action in a traffic class, use the **no** form of this command.

drop [**all**]

no drop [**all**]

Syntax Description

all	(Optional) Discards the entire stream of packets belonging to the traffic class.

Defaults

The packet discarding action in a traffic class is disabled.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Once the match criteria are applied to packets belonging to the specific traffic class using the **match class session** command in a class map, these packets can be discarded by configuring the **drop** command with the **all** keyword in a policy map. Packets match only on the packet session (flow) entry of the Flexible Packet Matching (FPM) access control list (ACL) pattern matching tool, and skip user-configured classification filters. When the **drop** command is specified with the **all** keyword, this command can only be associated with a class map that was created with the **class-map** command and **type access-control** keyword and used in a policy map that can be attached to one or more interfaces to specify a service policy that is created with the **policy-map** command and **type access-control** keyword.

Examples

The following example shows how to create and configure a traffic class called class1 for use in a policy map called **policy1**. The policy map (service policy) is attached to output serial interface 2/0. All packets that match access group 101 are placed in class1. Packets that belong to this class are discarded.

```
Router(config)# class-map class1
Router(config-cmap)# match access-group 101
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial2/0
Router(config-if)# service-policy output policy1
Router(config-if)# end
```

The following example shows how to configure a class map and policy map to specify the protocol stack class, the match criteria and action to take, and a combination of classes using session-based (flow-based) and nonsession-based actions. The **drop all** command is associated with the action to be taken on the policy.

```
Router(config)# class-map type access-control match-all my-HTTP
Router(config-cm)# match field tcp destport eq 8080
Router(config-cm)# match start tcp payload-start offset 20 size 10 regex "GET"

Router(config)# class-map type access-control match-all my-FTP
Router(config-cmap)# match field tcp destport eq 21

Router(config)# class-map type access-control match all class1
Router(config-cmap)# match class my-HTTP session
Router(config-cmap)# match start tcp payload-start offset 40 size 20 regex "abc.*def"

Router(config)# policy-map type access-control my_http_policy
Router(config-pmap)# class class1
Router(config-pmap-c)# drop all

Router(config)# interface gigabitEthernet 0/1
Router(config-if)# service-policy type access-control input my_http_policy
```

Related Commands

Command	Description
class	Specifies the name of a predefined traffic class, which was configured with the **class-map** command. The **class** command also classifies traffic to the traffic policy and enters policy-map class configuration mode.
class-map type access-control	Creates a class map to be used for matching packets to a specified class and enters class-map configuration mode for determining the exact pattern to look for in the protocol stack of interest.
log	Generates log messages for a predefined traffic class.
match class session	Configures match criteria for a class map used to identify a session (flow) containing packets of interest, which is then applied to all packets transmitted during the session.
policy-map type access-control	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy, and enters policy-map configuration mode.
show class-map	Displays all class maps and their matching criteria.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.

drop (zone-based policy)

To drop packets that are sent to the router, use the **drop** command in policy-map-class configuration mode.

drop [**log**]

Syntax Description

log	(Optional) Displays logging messages about dropped packets.

Command Default

Packets are not dropped.

Command Modes

Policy-map-class configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.1(1)S	This command was introduced into Cisco IOS Release 15.1(1)S.

Usage Guidelines

You can use this command only after entering the **policy-map type inspect** and **class type inspect** commands.

Examples

The following example creates an inspect policy map named p1 and specifies that packets will be dropped on the traffic at c1:

```
policy-map type inspect p1
 class type inspect c1
  drop
```

The following example defines a policy map that will drop HTTP traffic:

```
access-list 101 permit ip 192.168.1 0.0.0.255 any
 class-map type inspect match-all c1
  match access-group 101
  match protocol http
policy-map type inspect p1
 class type inspect c1
 drop
```

Related Commands

Command	Description
class type inspect	Specifies the traffic (class) on which an action is to be performed.
policy-map type inspect	Creates Layer 3 and Layer 4 inspect type policy maps.

dtls port

To configure a desired port for the Datagram Transport Layer Security (DTLS) to listen, use the **dtls port** command in WebVPN gateway configuration mode. To disable the port, use the **no** form of this command.

dtls port *port-number*

no dtls port *port-number*

Syntax Description

port-number	DTLS port number. Range: 1025 to 65535. Default: 443.

Command Default

The default DTLS port is 443.

Command Modes

WebVPN gateway configuration (config-webvpn-gateway)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

DTLS listens on port 443 by default. You can configure the desired DTLS port using the **dtls port** command.

Examples

The following example shows how to configure 1055 as the DTLS port for a WebVPN gateway "gateway1":

```
Router# configure terminal
Router(config)# webvpn gateway gateway1
Router(config-webvpn-gateway)# dtls port 1055
```

Related Commands

Command	Description
svc dtls	Enables DTLS support on the Cisco IOS SSL VPN.

dynamic

To define a named dynamic IP access list, use the **dynamic** command in access-list configuration mode. To remove the access lists, use the **no** form of this command.

dynamic *dynamic-name* [**timeout** *minutes*] {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**log**] [**fragments**]

no dynamic *dynamic-name*

Internet Control Message Protocol (ICMP)

dynamic *dynamic-name* [**timeout** *minutes*] {**deny** | **permit**} **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* [*icmp-code*] | *icmp-message*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**fragments**]

Internet Group Management Protocol (IGMP)

dynamic *dynamic-name* [**timeout** *minutes*] {**deny** | **permit**} **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**fragments**]

Transmission Control Protocol (TCP)

dynamic *dynamic-name* [**timeout** *minutes*] {**deny** | **permit**} **tcp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**fragments**]

User Datagram Protocol (UDP)

dynamic *dynamic-name* [**timeout** *minutes*] {**deny** | **permit**} **udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**fragments**]

Syntax Description

dynamic-name	Identifies this access list as a dynamic access list. Refer to lock-and-key access documented in the "Configuring Lock-and-Key Security (Dynamic Access Lists)" chapter in the *Cisco IOS Security Configuration Guide*.
timeout *minutes*	(Optional) Specifies the absolute length of time (in minutes) that a temporary access-list entry can remain in a dynamic access list. The default is an infinite length of time and allows an entry to remain permanently. Refer to lock-and-key access documented in the "Configuring Lock-and-Key Security (Dynamic Access Lists)" chapter in the *Cisco IOS Security Configuration Guide*.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
protocol	Name or number of an Internet protocol. It can be one of the keywords **eigrp**, **gre**, **icmp**, **igmp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, or **udp**, or an integer in the range from 0 to 255 representing an Internet protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the **ip** keyword. Some protocols allow further qualifiers described later.

source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part, dotted decimal format. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
source-wildcard	Wildcard bits to be applied to source. There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part, dotted decimal format. Place 1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part, dotted decimal format. • Use the **any** keyword as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place 1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
precedence *precedence*	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7, or by name as listed in the section “Usage Guidelines.”
tos *tos*	(Optional) Packets can be filtered by type of service (ToS) level, as specified by a number from 0 to 15, or by name as listed in the section “Usage Guidelines.”

log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.
fragments	(Optional) The access-list entry applies to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the "Access List Processing of Fragments" and "Fragments and Policy Routing" sections in the "Usage Guidelines" section.
icmp-type	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
icmp-code	(Optional) ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
icmp-message	(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name. The possible names are found in the section "Usage Guidelines."
igmp-type	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the section "Usage Guidelines."
operator	(Optional) Compares source or destination ports. Possible operands include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source* and *source-wildcard*, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard*, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number.
port	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the section "Usage Guidelines" of the **access-list** (IP extended) command. TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.

Defaults

An extended access list defaults to a list that denies everything. An extended access list is terminated by an implicit deny statement.

Command Modes

Access-list configuration

Command History

Release	Modification
11.2	This command was introduced.
12.0(11)	The **fragments** keyword was added.
12.2(13)T	The **igrp** keyword was removed because the IGRP protocol is no longer available in Cisco IOS software.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can use named access lists to control the transmission of packets on an interface and restrict contents of routing updates. The Cisco IOS software stops checking the extended access list after a match occurs.

Fragmented IP packets, other than the initial fragment, are immediately accepted by any extended IP access list. Extended access lists used to control vty access or restrict the contents of routing updates must not match against the TCP source port, the ToS value, or the precedence of the packet.

Note Named IP access lists will not be recognized by any software release prior to Cisco IOS Release 11.2.

Note After an access list is created, any subsequent additions (possibly entered from the terminal) are placed at the end of the list. In other words, you cannot selectively add or remove access list command lines from a specific access list.

The following is a list of precedence names:

- **critical**
- **flash**
- **flash-override**
- **immediate**
- **internet**
- **network**
- **priority**
- **routine**

The following is a list of ToS names:

- **max-reliability**
- **max-throughput**

- **min-delay**
- **min-monetary-cost**
- **normal**

The following is a list of ICMP message type and code names:

- **administratively-prohibited**
- **alternate-address**
- **conversion-error**
- **dod-host-prohibited**
- **dod-net-prohibited**
- **echo**
- **echo-reply**
- **general-parameter-problem**
- **host-isolated**
- **host-precedence-unreachable**
- **host-redirect**
- **host-tos-redirect**
- **host-tos-unreachable**
- **host-unknown**
- **host-unreachable**
- **information-reply**
- **information-request**
- **mask-reply**
- **mask-request**
- **mobile-redirect**
- **net-redirect**
- **net-tos-redirect**
- **net-tos-unreachable**
- **net-unreachable**
- **network-unknown**
- **no-room-for-option**
- **option-missing**
- **packet-too-big**
- **parameter-problem**
- **port-unreachable**
- **precedence-unreachable**
- **protocol-unreachable**
- **reassembly-timeout**
- **redirect**

- **router-advertisement**
- **router-solicitation**
- **source-quench**
- **source-route-failed**
- **time-exceeded**
- **timestamp-reply**
- **timestamp-request**
- **traceroute**
- **ttl-exceeded**
- **unreachable**

The following is a list of IGMP message names:

- **dvmrp**
- **host-query**
- **host-report**
- **pim**
- **trace**

The following is a list of TCP port names that can be used instead of port numbers. Refer to the current assigned numbers RFC to find a reference to these protocols. Port numbers corresponding to these protocols can also be found if you type a ? in the place of a port number.

- **bgp**
- **chargen**
- **daytime**
- **discard**
- **domain**
- **echo**
- **finger**
- **ftp**
- **ftp-data**
- **gopher**
- **hostname**
- **irc**
- **klogin**
- **kshell**
- **lpd**
- **nntp**
- **pop2**
- **pop3**
- **smtp**

- **sunrpc**
- **syslog**
- **tacacs-ds**
- **talk**
- **telnet**
- **time**
- **uucp**
- **whois**
- **www**

The following is a list of UDP port names that can be used instead of port numbers. Refer to the current assigned numbers RFC to find a reference to these protocols. Port numbers corresponding to these protocols can also be found if you type a ? in the place of a port number.

- **biff**
- **bootpc**
- **bootps**
- **discard**
- **dns**
- **dnsix**
- **echo**
- **mobile-ip**
- **nameserver**
- **netbios-dgm**
- **netbios-ns**
- **ntp**
- **rip**
- **snmp**
- **snmptrap**
- **sunrpc**
- **syslog**
- **tacacs-ds**
- **talk**
- **tftp**
- **time**
- **who**
- **xdmcp**

Access List Processing of Fragments

The behavior of access-list entries regarding the use or lack of the **fragments** keyword can be summarized as follows:

If the Access-List Entry has...	Then..
...no **fragments** keyword (the default behavior), and assuming all of the access-list entry information matches,	For an access-list entry containing only Layer 3 information: • The entry is applied to nonfragmented packets, initial fragments and noninitial fragments. For an access-list entry containing Layer 3 and Layer 4 information: • The entry is applied to nonfragmented packets and initial fragments. – If the entry is a **permit** statement, the packet or fragment is permitted. – If the entry is a **deny** statement, the packet or fragment is denied. • The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access-list entry can be applied. If the Layer 3 portion of the access-list entry matches, and – If the entry is a **permit** statement, the noninitial fragment is permitted. – If the entry is a **deny** statement, the next access-list entry is processed. **Note** The **deny** statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.
...the **fragments** keyword, and assuming all of the access-list entry information matches,	**Note** The access-list entry is applied only to noninitial fragments.The **fragments** keyword cannot be configured for an access-list entry that contains any Layer 4 information.

Be aware that you should not simply add the **fragments** keyword to every access-list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments** keyword, the packet is compared to the next access-list entry, and so on, until it is either permitted or denied by an access-list entry that does not contain the **fragments** keyword. Therefore, you may need two access-list entries for every **deny** entry. The first **deny** entry of the pair will not include the **fragments** keyword, and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases where there are multiple **deny** access-list entries for the same host but with different Layer 4 ports, a single **deny** access-list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets and each counts individually as a packet in access list accounting and access list violation counts.

Note The **fragments** keyword cannot solve all cases involving access lists and IP fragments.

Fragments and Policy Routing

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip address** command and the access list had entries that match on Layer 4 through 7 information. It is possible that noninitial fragments pass the access list and are policy routed, even if the first fragment was not policy routed or the reverse.

By using the **fragments** keyword in access-list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made and it is more likely policy routing will occur as intended.

Examples

The following example defines a dynamic access list named abclist:

```
ip access-group abclist in
!
ip access-list extended abclist
 dynamic testlist timeout 5
 permit ip any any
 permit tcp any host 10.302.21.2 eq 23
```

Related Commands

Command	Description
clear access-template	Clears a temporary access-list entry from a dynamic access list manually.
distribute-list in (IP)	Filters networks received in updates.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
ip access-group	Controls access to an interface.
ip access-list	Defines an IP access list by name.
logging console	Limits messages logged to the console based on severity.
show access-lists	Displays the contents of current IP and rate-limit access lists.
show ip access-list	Displays the contents of all current IP access lists.

eap

Note This command is removed effective with Cisco IOS Release 12.4(6)T.

To specify Extensible Authentication Protocol- (EAP-) specific parameters, use the **eap** command in identity profile configuration mode. To disable the parameters that were set, use the **no** form of this command.

eap {**username** *name* | **password** *password*}

no eap {**username** *name* | **password** *password*}

Syntax Description

username *name*	Username that will be sent to Request-Id packets.
password *password*	Password that should be used when replying to an Message Digest 5 (MD5) challenge.

Defaults

EAP parameters are not set.

Command Modes

Identity profile configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.4(6)T	This command was removed.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command if your router is configured as a supplicant. This command provides the means for configuring the identity and the EAP MD5 password that will be used by 802.1X to authenticate.

Examples

The following example shows that the EAP username “user1” has been configured:

```
Router (config)# identity profile dot1x
Router (config-identity-prof)# eap username user1
```

Related Commands

Command	Description
identity profile	Creates an identity profile.

eap (IKEv2 profile)

To derive the name mangler from the remote identity of type Extensible Authentication Protocol (EAP), use the **eap** command in IKEv2 name mangler configuration mode. To remove the name derived from EAP, use the **no** form of this command.

eap {**all** | **dn** {**common-name** | **country** | **domain** | **locality** | **organization** | **organization-unit** | **state**} {**prefix** | **suffix** {**delimiter** {**.** | **@** | ****}}}

no eap

Syntax Description

all	Derives the name mangler from the entire EAP identity.
dn	Derives the name from identities of type DN in EAP.
common-name	Derives the name from the common name portion in the DN.
country	Derives the name from the country name specified in the DN.
domain	Derives the name from the domain name specified in the DN.
locality	Derives the name from the locality specified in the DN.
organization	Derives the name from the organization specified in the DN.
organization-unit	Derives the name from the organization-unit specified in the DN.
state	Derives the name from the state name specified in the DN.
prefix	Derives the name from the prefix in EAP.
suffix	Derives the name from the suffix in EAP.
delimiter {**.** | **@** | ****}	Refers to the specified delimiter in the prefix or suffix.

Command Default

No default behavior or values.

Command Modes

IKEv2 name mangler configuration (config-ikev2-name-mangler)

Command History

Release	Modification
15.1(3)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to derive the name mangler from any field in the remote identity of type EAP.

Examples

The following example shows how to derive a name for the name mangler from a specific delimiter in EAP prefix:

```
Router(config)# crypto ikev2 name-mangler mangler2
Router(config-ikev2-name-mangler)# eap prefix delimiter @
```

Related Commands

Command	Description
crypto ikev2 name mangler	Defines a name mangler.

eckeypair

To configure the trustpoint to use an Elliptic Curve (EC) key on which certificate requests are generated using ECDSA signatures, use the **eckeypair** command in ca-trustpoint configuration mode. To remove the encryption key, use the **no** form of this command.

eckeypair *label*

no eckeypair *label*

Syntax Description

label	Specifies the EC key label that is configured using the **crypto key generate rsa** or **crypto key generate ec keysize** command in global configuration mode. See the Configuring Internet Key Exchange for IPsec VPNs feature module for more information.

Command Default

The trustpoint is not configured with an EC key.

Command Modes

Ca-trustpoint configuration mode (ca-trustpoint)

Command History

Release	Modification
15.1(2)T	This command was introduced in Cisco IOS Release 15.1(2)T.

Usage Guidelines

If an ECDSA signed certificate is imported without a trustpoint configuration, then the label defaults to the FQDN value.

Examples

The following example configures the EC key label in a certificate enrollment in a PKI:

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# eckeypair Router_1_Key
```

Related Commands

Command	Description
crypto key generate ec keysize	Generates EC keys.
crypto key generate rsa	Generates RSA keys.
crypto pki trustpoint	Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.

email (IKEv2 profile)

To derive the name mangler from the remote identity of type e-mail, use the **email** command in IKEv2 name mangler configuration mode. To remove the name derived from the e-mail, use the **no** form of this command.

email {**all** | **domain** | **username**}

no email

Syntax Description

all	Derives the name mangler from the entire FQDN.
domain	Derives the name mangler from the domain name in e-mail.
hostname	Derives the name mangler from the username in e-mail.

Command Default

No default behavior or values.

Command Modes

IKEv2 name mangler configuration (config-ikev2-name-mangler)

Command History

Release	Modification
15.1(3)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to derive the name mangler from any field in the remote identity of type e-mail.

Examples

The following example shows how to derive a name for the name mangler from the username in e-mail:

```
Router(config)# crypto ikev2 name-mangler mangler2
Router(config-ikev2-name-mangler)# email username
```

Related Commands

Command	Description
crypto ikev2 name mangler	Defines a name mangler.

enable

To change the privilege level for a CLI session or to use a CLI view for a CLI session, use the **enable** command in either user EXEC, privileged EXEC, or diagnostic mode.

enable [*privilege-level*] [**view** [*view-name*]]

Syntax Description

privilege-level	(Optional) Privilege level at which to log in.
view	(Optional) Enters into root view, which enables users to configure CLI views. **Note** This keyword is required if you want to configure a CLI view.
view-name	(Optional) Enters or exits a specified command-line interface (CLI) view. This keyword can be used to switch from one CLI view to another CLI view.

Defaults

Privilege-level 15 (privileged EXEC)

Command Modes

User EXEC (>)

Privileged EXEC (#)

Diagnostic Mode (diag)

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	The **view** keyword and *view-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **view** keyword and *view-name* argument were integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(22)SB.
Cisco IOS XE Release 2.1	This command became available on the ASR 1000 Series Routers, and became available in diagnostic mode for the first time.

Usage Guidelines

By default, using the **enable** command without the *privilege-level* argument in user EXEC mode causes the router to enter privileged EXEC mode (privilege-level 15).

Entering privileged EXEC mode enables the use of privileged commands. Because many of the privileged commands set operating parameters, privileged access should be password-protected to prevent unauthorized use. If the system administrator has set a password with the **enable password** global configuration command, you are prompted to enter the password before being allowed access to privileged EXEC mode. The password is case sensitive.

If an **enable** password has not been set, only enable mode can be accessed through the console connection.

Security levels can be set by an administrator using the **enable password** and **privilege level** commands. Up to 16 privilege levels can be specified, using the numbers 0 through 15. Using these privilege levels, the administrator can allow or deny access to specific commands. Privilege level 0 is associated with user EXEC mode, and privilege level 15 is associated with privileged EXEC mode.

For more information on defined privilege levels, see the *Cisco IOS Security Configuration Guide* and the *Cisco IOS Security Command Reference* publications.

If a level is not specified when entering the **enable** command, the user will enter the default mode of privileged EXEC (level 15).

Accessing a CLI View

CLI views restrict user access to specified CLI and configuration information. To configure and access CLI views, users must first enter into root view, which is accomplished via the **enable view** command (without the *view-name* argument). Thereafter, users are prompted for a password, which is the same password as the privilege level 15 password.

The *view-name* argument is used to switch from one view to another view.

To prevent dictionary attacks, a user is prompted for a password even if an incorrect view name is given. The user is denied access only after an incorrect view name and password are given.

Examples

In the following example, the user enters privileged EXEC mode (changes to privilege-level 15) by using the **enable** command without a privilege-level argument. The system prompts the user for a password before allowing access to the privileged EXEC mode. The password is not printed to the screen. The user then exits back to user EXEC mode using the **disable** command. Note that the prompt for user EXEC mode is the greater than symbol (>), and the prompt for privileged EXEC mode is the number sign (#).

```
Router> enable
Password: <letmein>
Router# disable
Router>
```

The following example shows which commands are available inside the CLI view “first” after the user has logged into this view:

```
Router# enable view first

Password:

00:28:23:%PARSER-6-VIEW_SWITCH:successfully set to view 'first'.
Router# ?
Exec commands:
  configure  Enter configuration mode
  enable     Turn on privileged commands
  exit       Exit from the EXEC
  show       Show running system information

Router# show ?

  ip       IP information
  parser   Display parser information
  version  System hardware and software status

Router# show ip ?

  access-lists            List IP access lists
```

```
  accounting              The active IP accounting database
  aliases                 IP alias table
  arp                     IP ARP table
  as-path-access-list     List AS path access lists
  bgp                     BGP information
  cache                   IP fast-switching route cache
  casa                    display casa information
  cef                     Cisco Express Forwarding
  community-list          List community-list
  dfp                     DFP information
  dhcp                    Show items in the DHCP database
  drp                     Director response protocol
  dvmrp                   DVMRP information
  eigrp                   IP-EIGRP show commands
  extcommunity-list       List extended-community list
  flow                    NetFlow switching
  helper-address          helper-address table
  http                    HTTP information
  igmp                    IGMP information
  irdp                    ICMP Router Discovery Protocol
.
.
```

The following example shows how to use the **enable view** command to switch from the root view to the CLI view “first”:

```
Router# enable view
Router#
01:08:16:%PARSER-6-VIEW_SWITCH:successfully set to view 'root'.
Router#
! Enable the show parser view command from the root view
Router# show parser view

Current view is 'root'
! Enable the show parser view command from the root view to display all views
Router# show parser view all

Views Present in System:
View Name:   first
View Name:   second
! Switch to the CLI view “first.”
Router# enable view first
Router#
01:08:09:%PARSER-6-VIEW_SWITCH:successfully set to view 'first'.
! Enable the show parser view command from the CLI view “first.”
Router# show parser view

Current view is 'first'
```

Related Commands

Command	Description
disable	Exits from privileged EXEC mode to user EXEC mode, or, if privilege levels are set, to the specified privilege level.
enable password	Sets a local password to control access to various privilege levels.
privilege level (global)	Sets a privilege level for a command.
privilege level (line)	Sets a privilege level for a command for a specific line.

enable password

To set a local password to control access to various privilege levels, use the **enable password** command in global configuration mode. To remove the password requirement, use the **no** form of this command.

enable password [**level** *level*] {*password* | [*encryption-type*] *encrypted-password*}

no enable password [**level** *level*]

Syntax Description

level *level*	(Optional) Level for which the password applies. You can specify up to 16 privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges. If this argument is not specified in the command or the **no** form of the command, the privilege level defaults to 15 (traditional enable privileges).
password	Password users type to enter enable mode.
encryption-type	(Optional) Cisco-proprietary algorithm used to encrypt the password. Currently the only encryption type available is 5. If you specify *encryption-type*, the next argument you supply must be an encrypted password (a password already encrypted by a Cisco router).
encrypted-password	Encrypted password you enter, copied from another router configuration.

Defaults

No password is defined. The default is level 15.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Caution If neither the **enable password** command nor the **enable secret** command is configured, and if there is a line password configured for the console, the console line password will serve as the enable password for all VTY (Telnet and Secure Shell [SSH]) sessions.

Use this command with the **level** option to define a password for a specific privilege level. After you specify the level and the password, give the password to the users who need to access this level. Use the **privilege level** configuration command to specify commands accessible at various levels.

You will not ordinarily enter an encryption type. Typically you enter an encryption type only if you copy and paste into this command a password that has already been encrypted by a Cisco router.

Caution If you specify an encryption type and then enter a clear text password, you will not be able to reenter enable mode. You cannot recover a lost password that has been encrypted by any method.

If the **service password-encryption** command is set, the encrypted form of the password you create with the **enable password** command is displayed when a **more nvram:startup-config** command is entered.

You can enable or disable password encryption with the **service password-encryption** command.

An enable password is defined as follows:

- Must contain from 1 to 25 uppercase and lowercase alphanumeric characters.
- Must not have a number as the first character.
- Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.
- Can contain the question mark (?) character if you precede the question mark with the key combination Crtl-v when you create the password; for example, to create the password *abc?123,* do the following:
  - Enter **abc**.
  - Type **Crtl-v**.
  - Enter **?123**.

  When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-v; you can simply enter abc?123 at the password prompt.

Examples

The following example enables the password “pswd2” for privilege level 2:

```
enable password level 2 pswd2
```

The following example sets the encrypted password “1i5Rkls3LoyxzS8t9”, which has been copied from a router configuration file, for privilege level 2 using encryption type 7:

```
enable password level 2 5 $1$i5Rkls3LoyxzS8t9
```

Related Commands

Command	Description
disable	Exits privileged EXEC mode and returns to user EXEC mode.
enable	Enters privileged EXEC mode.
enable secret	Specifies an additional layer of security over the **enable password** command.
privilege	Configures a new privilege level for users and associate commands with that privilege level.
service password-encryption	Encrypts passwords.
show privilege	Displays your current level of privilege.

enable secret

To specify an additional layer of security over the **enable password** command, use the **enable secret** command in global configuration mode. To turn off the **enable secret** function, use the **no** form of this command.

enable secret [**level** *level*] {*password* **| 0 | 4 | 5** [*encryption-type*] *encrypted-password* **}**

no enable secret [**level** *level*] {*password* **| 0 | 4 | 5** [*encryption-type*] *encrypted-password* **}**

Syntax Description

level *level*	(Optional) Specifies the level for which the password applies. You can specify up to sixteen privilege levels, using the numerals 0 through 15. Level 1 is normal EXEC-mode user privileges. If the level argument is not specified in the command or in the **no** form of the command, the privilege level defaults to 15 (traditional enable privileges).
password	Password for users to enter enable mode. This password should be different from the password created with the **enable password** command.
0	Specifies an unencrypted clear-text password. The password is converted to a SHA256 secret and gets stored in the router.
4	Specifies an SHA256 encrypted secret string. The SHA256 secret string is copied from the router configuration.
5	Specifies a message digest alogrithm5 (MD5) encrypted secret.
encryption-type	(Optional) Cisco-proprietary algorithm used to encrypt the password. The encryption types available for this command are 4 and 5. If you specify a value for *encryption-type* argument, the next argument you supply must be an encrypted password (a password encrypted by a Cisco router).
encrypted-password	Encrypted password that is copied from another router configuration.

Command Default

No password is defined. The default level is 15.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S. Encryption types **0**, **4**, and **5** were added.

Usage Guidelines

Caution If neither the **enable password** command nor the **enable secret** command is configured, and if there is a line password configured for the console, the console line password will serve as the enable password for all vty (Telnet and Secure Shell [SSH]) sessions.

Use this command to provide an additional layer of security over the enable password. The **enable secret** command provides better security by storing the enable secret password using a non reversible cryptographic function. The added layer of security encryption provides is useful in environments where the password crosses the network or is stored on a TFTP server.

You will not ordinarily enter an encryption type. Typically you enter an encryption type only if you paste into this command an encrypted password that you copied from a router configuration file.

Caution If you specify an encryption type and then enter a clear-text password, you will not be able to reenter enable mode. You cannot recover a lost password that has been encrypted by any method.

If you use the same password for the **enable password** and **enable secret** commands, you receive an error message warning that this practice is not recommended, but the password will be accepted. By using the same password, however, you undermine the additional security the **enable secret** command provides.

Note After you set a password using the **enable secret** command, a password set using the **enable password** command works only if the **enable secret** is disabled or an older version of Cisco IOS software is being used, such as when running an older rxboot image. Additionally, you cannot recover a lost password that has been encrypted by any method.

If **service password-encryption** is set, the encrypted form of the password you create here is displayed when a **more nvram:startup-config** command is entered.

You can enable or disable password encryption with the **service password-encryption** command.

An enable password is defined as follows:

- Must contain from 1 to 25 uppercase and lowercase alphanumeric characters
- Must not have a number as the first character
- Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.
- Can contain the question mark (?) character if you precede the question mark with the key combination Crtl-v when you create the password; for example, to create the password *abc?123,* do the following:
  - Enter **abc**.
  - Type **Crtl-v**.
  - Enter **?123**.

  When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-v; you can simply enter **abc?123** at the password prompt.

Examples

The following example specifies the enable secret password of “password”:

```
enable secret password
```

After specifying an enable secret password, users must enter this password to gain access. Any passwords set through enable password will no longer work.

```
Password: password
```

The following example enables the encrypted password "1FaD0$Xyti5Rkls3LoyxzS8", which has been copied from a router configuration file, for privilege level 2 using encryption type 5:

```
enable password level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

Related Commands

Command	Description
enable	Enters privileged EXEC mode.
enable password	Sets a local password to control access to various privilege levels.
service password-encryption	Encrypt passwords.

enabled (IPS)

To change the enabled status of a given signature or signature category, use the **enabled** command in signature-definition-status (config-sigdef-status) or IPS-category-action (config-ips-category-action) configuration mode. To return to the default action, use the **no** form of this command.

enabled {**true** | **false**}

no enabled

Syntax Description

true	Enables a specified signature or all signatures within a specified category.
false	Disables a specified signature or all signatures within a specified category.

Command Default

All commands are enabled.

Command Modes

Signature-definition-status configuration (config-sigdef-status)
IPS-category-action configuration (config-ips-category-action)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use the **enabled** command to change the status of a signature or signature category to active (true) or inactive (false).

Examples

The following example shows how to change the status of signature 9000:0 to enabled:

```
Router(config)# ip ips signature-definition
Router(config-sig)# signature 9000 0
Router(config-sig-sig)# status
Router(config-sigdef-status)# enabled true
```

Related Commands

Command	Description
category	Specifies a signature category that is to be used for multiple signature actions or conditions.
signature	Specifies a signature for which the CLI user tunings will be changed.
status	Changes the enabled or retired status of a given signature or signature category.

encryption (IKE policy)

To specify the encryption algorithm within an Internet Key Exchange (IKE) policy, use the **encryption** command in Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the encryption algorithm to the default value, use the **no** form of this command.

encryption {**des** | **3des** | **aes** | **aes 192** | **aes 256**}

no encryption

Syntax Description

des	56-bit Data Encryption Standard (DES)-CBC as the encryption algorithm.
3des	168-bit DES (3DES) as the encryption algorithm.
aes	128-bit Advanced Encryption Standard (AES) as the encryption algorithm.
aes 192	192-bit AES as the encryption algorithm.
aes 256	256-bit AES as the encryption algorithm.

Command History

The 56-bit DES-CBC encryption algorithm

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.0(2)T	The **3des** option was added.
12.2(13)T	The following keywords were added: **aes**, **aes 192**, and **aes 256**.
12.4(4)T	IPv6 support was added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to specify the encryption algorithm to be used in an IKE policy.

If a user enters an IKE encryption method that the hardware does not support, a warning message will be displayed immediately after the **encryption** command is entered.

Examples

The following example configures an IKE policy with the 3DES encryption algorithm (all other parameters are set to the defaults):

```
crypto isakmp policy
 encryption 3des
 exit
```

The following example is a sample warning message that is displayed when a user enters an IKE encryption method that the hardware does not support:

```
encryption aes 256
WARNING:encryption hardware does not support the configured
    encryption method for ISAKMP policy 1
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
group (IKE policy)	Specifies the DH group identifier within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
show crypto isakmp policy	Displays the parameters for each IKE policy.

encryption (IKEv2 proposal)

To specify one or more encryption algorithms for an Internet Key Exchange Version 2 (IKEv2) proposal, use the **encryption** command in IKEv2 proposal configuration mode. To remove the encryption algorithm, use the **no** form of this command.

encryption {**3des**} {**aes-cbc-128**} {**aes-cbc-192**} {**aes-cbc-256**}

no encryption

Syntax Description

3des	Specifies 168-bit DES (3DES) as the encryption algorithm.
aes-cbc-128	Specifies 128-bit Advanced Encryption Standard-Cipher Block Chaining (AES-CBC) as the encryption algorithim.
aes-cbc-192	Specifies 192-bit AES-CBC as the encryption algorithim.
aes-cbc-256	Specifies 256-bit AES-CBC as the encryption algorithim.

Command Default

The encryption algorithm is not specified.

Command Modes

IKEv2 proposal configuration (config-ikev2-proposal)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to specify the encryption algorithm to be used in an IKEv2 proposal. The default encryption algorithm in the default proposal is 128-bit AES-CBC and 3 DES encryption algorithm.

Note You cannot selectively remove an encryption algorithm when multiple encryption algorithms are configured.

Examples

The following example configures an IKE proposal with the 3DES encryption algorithm:

```
Router(config)# crypto ikev2 proposal proposal1
Router(config-ikev2-proposal)# encryption 3des
```

Related Commands

Command	Description
crypto ikev2 proposal	Defines an IKEv2 proposal.
group (ikev2 proposal)	Specifies the DH group identifier in an IKEv2 proposal.

Command	Description
integrity (ikev2 proposal)	Specifies the integrity algorithm in an IKEv2 proposal.
show crypto ikev2 proposal	Displays the parameters for each IKEv2 proposal.

enforce-checksum

To enforce checksum verification for Flexible Packet Matching (FPM), use the **enforce-checksum** command in fpm package-info mode. To disable the checksum verification, use the **no** form of this command.

enforce-checksum

no enforce-checksum

Syntax Description

This command has no keywords and arguments.

Command Default

enforce checksum is enabled.

Command Modes

fpm package-info (config-fpm-pak-info)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **enforce-checksum** command ensures that the FPM verifies the checksum of the package during load and that the package has not been tampered. This command is useful when you want to define your own filters inside the FPM packages by disabling enforce-checksum using **no enforce-checksum** command. However, it is recommended to keep the **enforce-checksum** enabled.

Examples

The following example shows how to enable the **enforce-checksum** command:

```
Router# configure terminal
Router(config)# fpm package-info
Router(config-fpm-pak-info)# enforce-checksum
```

engine (IPS)

To enter signature-definition-action-engine configuration mode, which allows you to change router actions for a specified signature, use the **engine** command in signature-definition-action configuration mode.

engine

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Signature-definition-action configuration (config-sigdef-action)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

If you wish to change router actions for a specific signature, you must issue the engine command to enter the appropriate configuration mode, which allows you to issue the **event-action** command and specify any supported action.

Examples

The following example shows how to configure signature 5726 to reset all TCP connections and produce an alert:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ips signature-definition
Router(config-sigdef)# signature 5726 0
Router(config-sigdef-sig)# engine
Router(config-sigdef-sig-engine)# event-action reset-tcp-connection produce-alert
Router(config-sigdef-sig-engine)# exit
Router(config-sigdef-sig)# exit
Router(config-sigdef)#^ZDo you want to accept these changes? [confirm]
Router#
*Nov 9 21:50:55.847: %IPS-6-ENGINE_BUILDING: multi-string - 3 signatures - 12 of 11
engines
*Nov 9 21:50:55.859: %IPS-6-ENGINE_READY: multi-string - build time 12 ms - packets for
this engine will be scanned
*Nov 9 21:50:55.859: %SYS-5-CONFIG_I: Configured from console by cisco on console
```

Related Commands

Command	Description
event-action	Changes router actions for a signature or signature category.
signature	Specifies a signature for which the CLI user tunings will be changed.

enrollment

To specify the enrollment parameters of your certification authority (CA), use the **enrollment** command in ca-trustpoint configuration mode. To remove any of the configured parameters, use the **no** form of this command.

enrollment {**mode ra** | **retry count** *number* | **retry period** *minutes* | **url** *url*}

no enrollment {**mode ra** | **retry count** *number* | **retry period** *minutes* | **url** *url*}

Syntax Description

mode ra	Specifies registration authority (RA) mode as the mode supported by the CA.
retry count *number*	Specifies the number of times that a router will resend a certificate request when it does not receive a response from the previous request. The range is from 1 to 100. The default is 10.
retry period *minutes*	Specifies the wait period between certificate request retries. The range is from 1 to 60.
url *url*	Specifies the URL of the CA where your router should send certificate requests.

Defaults

RA mode is disabled.

After the router sends the first certificate request to the CA, it waits for 1 minute before sending a second request. After the second request, the interval between requests (the retry period) increases exponentially, with an additional 1 minute interval added at each increment.

The router sends a maximum of ten requests.

Your router does not know the CA URL until you specify it using **url** *url*.

Command Modes

CA-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(13)T	The **url** *url* option was enhanced to support TFTP enrollment.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.

Usage Guidelines

Use the **mode** keyword to specify the mode supported by the CA. This keyword is required if your CA system provides an RA.

Use the **retry period** *minutes* option to change the retry period from the default value. After requesting a certificate, the router waits to receive a certificate from the CA. If the router does not receive a certificate within a period of time (the retry period), the router will send another certificate request. The router will continue to send requests until it receives a valid certificate, until the CA returns an enrollment error, or until the configured number of retries is exceeded.

By default, the router sends a maximum of ten requests; you can change this parameter using the **retry count** *number* option. It stops sending requests when it receives a valid certificate, when the CA returns an enrollment error, or when the configured number of requests is reached.

Use the **url** *url* option to specify or change the URL of the CA. You can specify enrollment with Simple Certificate Enrollment Protocol (SCEP) using a HTTP URl or with TFTP using a TFTP URL.

If you are using (SCEP) for enrollment, *url* must be in the form http://CA_name, where CA_name is the CA's host Domain Name System (DNS) name or IP address. If you are using TFTP for enrollment, *url* must be in the form tftp://certserver/file_specification.

TFTP enrollment is used to send the enrollment request and retrieve the certificate of the CA and the certificate of the router. If the file_specification is included in the URL, the router will append an extension onto the file specification. When the **crypto ca authenticate** command is entered, the router will retrieve the certificate of the CA from the specified TFTP server. As appropriate, the router will append the extension ".ca" to the filename or the fully qualified domain name (FQDN). If the **url** *url* option does not include a file specification, the router's FQDN will be used.

Note The **crypto ca trustpoint** command replaces the **crypto ca identity** and **crypto ca trusted-root** commands and all related subcommands (all ca-identity and trusted-root configuration mode commands). If you enter a ca-identity or trusted-root subcommand, the configuration mode and command will be written back as ca-trustpoint.

Examples

The following example shows how to declare a CA named ka and how to specify registration authority mode. It also shows how to set a retry count of 8 and a retry period of 2 minutes:

```
Router(config)# crypto ca trustpoint ka
Router(ca-trustpoint)# enrollment mode ra
Router(ca-trustpoint)# enrollment retry count 8
Router(ca-trustpoint)# enrollment retry period 2
```

The following example shows how to declare a CA named ka and how to specify the URL of the CA as http://example:80:

```
Router(config)# crypto ca trustpoint ka
Router(ca-trustpoint)# enrollment url http://example:80
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the CA (by getting the CA's certificate).
crypto ca trustpoint	Declares the CA that your router should use.
enrollment command	Specifies the HTTP command that is sent to the CA for enrollment.
enrollment credential	Specifies an existing trustpoint from another vendor that is to be enrolled with the Cisco IOS certificate server.
enrollment http-proxy	Enables access to the CA by HTTP through the proxy server.
enrollment profile	Specifies that an enrollment profile can be used for certificate authentication and enrollment.
enrollment selfsigned	Specifies self-signed enrollment for a trustpoint.
enrollment terminal	Specifies manual cut-and-paste certificate enrollment.
enrollment url	Specifies the enrollment parameters of a CA.

enrollment command

To specify the HTTP command that is sent to the certification authority (CA) for enrollment, use the **enrollment command** command in ca-profile-enroll configuration mode.

enrollment command

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Ca-profile-enroll configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

After enabling this command, you can use the **parameter** command to specify enrollment parameters for your enrollment profile.

Examples

The following example shows how to configure the enrollment profile name “E” for certificate enrollment:

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial

crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
crypto ca profile enrollment	Defines an enrollment profile.
parameter	Specifies parameters for an enrollment profile.

enrollment credential

To specify an existing trustpoint from another vendor that is to be enrolled with the Cisco IOS certificate server, use the **enrollment credential** command in ca-profile-enroll configuration mode.

enrollment credential *label*

Syntax Description

label	Name of the certification authority (CA) trustpoint of another vendor.

Defaults

No default behavior or values.

Command Modes

Ca-profile-enroll configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

To configure a router that is already enrolled with a CA of another vendor that is to be enrolled with a Cisco IOS certificate server, you must configure a certificate enrollment profile (via the **crypto pki profile enrollment** command). Thereafter, you should issue the **enrollment credential** command, which specifies the trustpoint of another vendor that has to be enrolled with a Cisco IOS certificate server.

Examples

The following example shows how to configure a client router and a Cisco IOS certificate server to exchange enrollment requests via a certificate enrollment profile:

```
! Define the trustpoint "msca-root" that points to the non-Cisco IOS CA and enroll and
! authenticate the client with the non-Cisco IOS CA.
crypto pki trustpoint msca-root
 enrollment mode ra
 enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
 ip-address FastEthernet2/0
 revocation-check crl
!
! Configure trustpoint "cs" for Cisco IOS CA.
crypto pki trustpoint cs
 enrollment profile cs1
 revocation-check crl
!
! Define enrollment profile "cs1," which points to Cisco IOS CA and mention (via the
! enrollment credential command) that "msca-root" is being initially enrolled with the
! Cisco IOS CA.
crypto pki profile enrollment cs1
 enrollment url  http://cs:80
 enrollment credential  msca-root!
```

```
! Configure the certificate server, and issue and the grant auto trustpoint command to
! instruct the certificate server to accept enrollment request only from clients who are
! already enrolled with trustpoint "msca-root."
crypto pki server cs
 database level minimum
 database url nvram:
 issuer-name CN=cs
 grant auto trustpoint msca-root
!
crypto pki trustpoint cs
 revocation-check crl
rsakeypair cs
!
crypto pki trustpoint msca-root
 enrollment mode ra
 enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
 revocation-check crl
```

Related Commands

Command	Description
crypto pki profile enrollment	Defines an enrollment profile.

enrollment http-proxy

To access the certification authority (CA) by HTTP through the proxy server, use the **enrollment http-proxy** command in ca-trustpoint configuration mode.

enrollment http-proxy *host-name port-num*

Syntax Description

host-name	Defines the proxy server used to get the CA.
port-num	Specifies the port number used to access the CA.

Defaults

If this command is not enabled, the CA will not be accessed via HTTP.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.

Usage Guidelines

The **enrollment http-proxy** command must be used in conjunction with the **enrollment** command, which specifies the enrollment parameters for the CA.

Examples

The following example shows how to access the CA named “ka” by HTTP through the bomborra proxy server:

```
crypto ca trustpoint ka
 enrollment url http://kahului
 enrollment http-proxy bomborra 8080
 crl optional
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
enrollment	Specifies the enrollment parameters of your CA.

enrollment mode ra

The **enrollment mode ra** command is replaced by the **enrollment command** command. See the **enrollment command** command for more information.

enrollment profile

To specify that an enrollment profile can be used for certificate authentication and enrollment, use the **enrollment profile** command in ca-trustpoint configuration mode. To delete an enrollment profile from your configuration, use the **no** form of this command.

enrollment profile *label*

no enrollment profile *label*

Syntax Description

label	Creates a name for the enrollment profile.

Defaults

Your router does not recognize any enrollment profiles until you declare one using this command.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

Before you can enable this command, you must enter the **crypto ca trustpoint** command.

The **enrollment profile** command enables your router to accept an enrollment profile, which can be configured via the **crypto ca profile enrollment** command. The enrollment profile, which consists of two templates, can be used to specify different URLs or methods for certificate authentication and enrollment.

Examples

The following example shows how to declare the enrollment profile named “E”:

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial

crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
crypto ca profile enrollment	Defines an enrollment profile.
crypto ca trustpoint	Declares the CA that your router should use.

enrollment retry count

The **enrollment retry count** command is replaced by the **enrollment** command. See the **enrollment** command for more information.

enrollment retry period

The **enrollment retry period** command is replaced by the **enrollment** command. See the **enrollment** command for more information.

enrollment selfsigned

To specify self-signed enrollment for a trustpoint, use the **enrollment selfsigned** command in ca-trustpoint configuration mode. To delete self-signed enrollment from a trustpoint, use the **no** form of this command.

enrollment selfsigned

no enrollment selfsigned

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default behavior or values.

Command Modes

ca-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Before you can use the **enrollment selfsigned** command, you must enable the **crypto pki trustpoint** command, which defines the trustpoint and enters ca-trustpoint configuration mode.

If you do not use this command, you should specify another enrollment method for the router by using an enrollment command such as **enrollment url** or **enrollment terminal**.

Examples

The following example shows a self-signed certificate being designated for a trustpoint named local:

```
crypto pki trustpoint local
 enrollment selfsigned
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the CA that your router should use.

enrollment terminal (ca-profile-enroll)

To specify manual cut-and-paste certificate enrollment, use the **enrollment terminal** command in ca-profile-enroll configuration mode. To delete a current enrollment request, use the **no** form of this command.

enrollment terminal

no enrollment terminal

Syntax Description

This command has no arguments or keywords.

Defaults

A certificate enrollment request is not specified.

Command Modes

Ca-profile-enroll configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

A user may manually cut-and-paste certificate authentication requests and certificates when a network connection between the router and certification authority (CA) is unavailable. After this command is enabled, the certificate request is printed on the console terminal so that it can be manually copied (cut) by the user.

Note Although most routers accept manual enrollment, the process can be tedious if a large number of routers have to be enrolled.

Examples

The following example shows how to configure the enrollment profile named "E" to perform certificate authentication via HTTP and manual certificate enrollment:

```
crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment terminal
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
crypto ca profile enrollment	Defines an enrollment profile.

enrollment terminal (ca-trustpoint)

To specify manual cut-and-paste certificate enrollment, use the **enrollment terminal** command in ca-trustpoint configuration mode. To delete a current enrollment request, use the **no** form of this command.

enrollment terminal [**pem**]

no enrollment terminal [**pem**]

Syntax Description

pem	(Optional) Adds privacy-enhanced mail (PEM) boundaries to the certificate request.

Defaults

No default behavior or values

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.3(4)T	The **pem** keyword was added.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

A user may want to manually cut-and-paste certificate requests and certificates when he or she does not have a network connection between the router and certification authority (CA). When this command is enabled, the router displays the certificate request on the console terminal, allowing the user to enter the issued certificate on the terminal.

The pem Keyword

Use the **pem** keyword to issue certificate requests (via the **crypto ca enroll** command) or receive issued certificates (via the **crypto ca import certificate** command) in PEM-formatted files through the console terminal. If the CA server does not support simple certificate enrollment protocol (SCEP), the certificate request can be presented to the CA server manually.

Note When generating certificate requests in PEM format, your router does not have to have the CA certificate, which is obtained via the **crypto ca authenticate** command.

Examples

The following example shows how to manually specify certificate enrollment via cut-and-paste. In this example, the CA trustpoint is "MS."

```
crypto ca trustpoint MS
 enrollment terminal
 crypto ca authenticate MS
!
crypto ca enroll MS
crypto ca import MS certificate
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the CA (by getting the certificate of the CA).
crypto ca enroll	Obtains the certificates of your router from the certification authority.
crypto ca import	Imports a certificate manually via TFTP or cut-and-paste at the terminal.
crypto ca trustpoint	Declares the CA that your router should use.

enrollment url (ca-identity)

The **enrollment url (ca-identity)** command is replaced by the **enrollment url (ca-trustpoint)** command. See the **enrollment url (ca-trustpoint)** command for more information.

enrollment url (ca-profile-enroll)

To specify the URL of the certification authority (CA) server to which to send enrollment requests, use the **enrollment url** command in ca-profile-enroll configuration mode. To delete the enrollment URL from your enrollment profile, use the **no** form of this command.

enrollment url *url*

no enrollment url *url*

Syntax Description

url	URL of the CA server to which your router should send certificate requests. If you are using Simple Certificate Enrollment Protocol (SCEP) for enrollment, the *url* argument must be in the form http://CA_name, where CA_name is the host Domain Name System (DNS) name or IP address of the CA. If you are using TFTP for enrollment, the *url* argument must be in the form tftp://certserver/file_specification. (If the URL does not include a file specification, the fully qualified domain name [FQDN] of the router will be used.)

Defaults

Your router does not recognize the CA URL until you specify it using this command.

Command Modes

Ca-profile-enroll configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

This command allows the user to specify a different URL or a different method for authenticating a certificate and enrolling a certificate; for example, manual authentication and TFTP enrollment.

Examples

The following example shows how to enable certificate enrollment via HTTP for the profile name “E”:

```
crypto pki trustpoint Entrust
  enrollment profile E
  serial

crypto pki profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
```

```
parameter 2 value 5001
```

Related Commands

Command	Description
crypto pki profile enrollment	Defines an enrollment profile.

enrollment url (ca-trustpoint)

To specify the enrollment parameters of a certification authority (CA), use the **enrollment url** command in ca-trustpoint configuration mode. To remove any of the configured parameters, use the **no** form of this command.

enrollment [**mode**] [**retry period** *minutes*] [**retry count** *number*] **url** *url* [**pem**]

no enrollment [**mode**] [**retry period** *minutes*] [**retry count** *number*] **url** *url* [**pem**]

Syntax Description

mode	(Optional) Specifies the registration authority (RA) mode, if your CA system provides an RA. By default, RA mode is disabled.
retry period *minutes*	(Optional) Specifies the period in which the router will wait before sending the CA another certificate request. The default is 1 minute between retries. (Specify from 1 to 60 minutes.)
retry count *number*	(Optional) Specifies the number of times a router will resend a certificate request when it does not receive a response from the previous request. The default is 10 retries. (Specify from 1 to 100 retries.)
url *url*	Specifies the URL of the file system where your router should send certificate requests. For enrollment method options, see Table 32.
pem	(Optional) Adds privacy-enhanced mail (PEM) boundaries to the certificate request.

Defaults

Your router does not know the CA URL until you specify it using the **url** *url* keyword and argument.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
11.3T	This command was introduced as the **enrollment url** (ca-identity) command.
12.2(8)T	This command replaced the **enrollment url** (ca-identity) command. The **mode**, **retry period** *minutes*, and **retry count** *number* keywords and arguments were added.
12.2(13)T	The **url** *url* option was enhanced to support TFTP enrollment.
12.3(4)T	The **pem** keyword was added, and the **url** *url* option was enhanced to support an additional enrollment method—the Cisco IOS File System (IFS).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

Use the **mode** keyword to specify the mode supported by the CA. This keyword is required if your CA system provides an RA.

Use the **retry period** *minutes* option to change the retry period from the default of 1 minute between retries. After requesting a certificate, the router waits to receive a certificate from the CA. If the router does not receive a certificate within a specified period of time (the retry period), the router will send another certificate request. By default, the router will send a maximum of ten requests until it receives a valid certificate, until the CA returns an enrollment error, or until the configured number of retries (specified via the **retry count** *number* option) is exceeded.

Use the **pem** keyword to issue certificate requests (using the **crypto pki enroll** command) or receive issued certificates (using the **crypto pki import certificate** command) in PEM-formatted files.

Note When generating certificate requests in PEM format, your router does not have to have the CA certificate, which is obtained using the **crypto ca authenticate** command.

Use the **url** *url* option to specify or change the URL of the CA. Table 32 lists the available enrollment methods.

Table 32 Certificate Enrollment Methods

Enrollment Method	Description
bootflash	Enroll via bootflash: file system
cns	Enroll via Cisco Networking Services (CNS): file system
flash	Enroll via flash: file system
ftp	Enroll via FTP: file system
null	Enroll via null: file system
nvram	Enroll via NVRAM: file system
rcp	Enroll via remote copy protocol (rcp): file system
scp	Enroll via secure copy protocol (scp): file system
SCEP[1]	Enroll via Simple Certificate Enrollment Protocol (SCEP) (an HTTP URL)
system	Enroll via system: file system
TFTP[2]	Enroll via TFTP: file system

1. If you are using SCEP for enrollment, the URL must be in the form http://CA_name, where CA_name is the host Domain Name System (DNS) name or IP address of the CA.
2. If you are using TFTP for enrollment, the URL must be in the form tftp://certserver/file_specification. (The file_specification is optional. See the section "TFTP Certificate Enrollment" for additional information.)

TFTP Certificate Enrollment

TFTP enrollment is used to send the enrollment request and retrieve the certificate of the CA and the certificate of the router. If the file_specification is included in the URL, the router will append an extension onto the file specification. When the **crypto pki authenticate** command is entered, the router will retrieve the certificate of the CA from the specified TFTP server. As appropriate, the router will append the extension ".ca" to the filename or the fully qualified domain name (FQDN). (If the **url** *url* option does not include a file specification, the FQDN of the router will be used.)

Note The **crypto pki trustpoint** command replaces the **crypto ca identity** and **crypto ca trusted-root** commands and all related commands (all **ca-identity** and **trusted-root** configuration mode commands). If you enter a **ca-identity** or **trusted-root** command, the configuration mode and command will be written back as pki-trustpoint.

Examples

The following example shows how to declare a CA named "trustpoint" and specify the URL of the CA as "http://example:80":

```
crypto pki trustpoint trustpoint
 enrollment url http://example:80
```

Related Commands

Command	Description
crypto pki authenticate	Authenticates the CA (by getting the certificate of the CA).
crypto pki enroll	Obtains the certificate or certificates of your router from the CA.
crypto pki trustpoint	Declares the CA that your router should use.

eou allow

To allow additional Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) options, use the **eou allow** command in global configuration mode. To disable the options that have been set, use the **no** form of this command.

eou allow {**clientless** | **ip-station-id**}

no eou allow {**clientless** | **ip-station-id**}

Syntax Description

clientless	Allows authentication of clientless hosts (systems that do not run Cisco Trust Agent).
ip-station-id	Allows an IP address in the station-id field.

Defaults

No additional EAPoUDP options are allowed.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

The **eou allow** command used with the **clientless** keyword requires that a user group be configured on the Cisco Access Control Server (ACS) using the same username and password that are specified using the **eou clientless** command.

Examples

The following example shows that clientless hosts are allowed:

```
Router (config)# eou allow clientless
```

Related Commands

Command	Description
eou clientless	Sets user group credentials for clientless hosts.

eou clientless

To set user group credentials for clientless hosts, use the **eou clientless** command in global configuration mode. To remove the user group credentials, use the **no** form of this command.

eou clientless {**password** *password* | **username** *username*}

no eou clientless {**password | username**}

Syntax Description

password *password*	Sets a password.
username *username*	Sets a username.

Defaults

Username and password values are clientless.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

For this command to be effective, the **eou allow** command must also be enabled.

Examples

The following example shows that a clientless host with the username “user1” has been configured:

```
Router (config)# eou clientless username user1
```

The following example shows that a clientless host with the password “user123” has been configured:

```
Router (config)# eou clientless password user123
```

Related Commands

Command	Description
eou allow	Allows additional EAPoUDP options.

eou default

To set global Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) parameters to the default values, use the **eou default** command in global or interface configuration mode.

eou default

Syntax Description

This command has no arguments or keywords.

Defaults

The EAPoUDP parameters are set to their default values.

Command Modes

Global configuration (config)
Interface configuration (config-if)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

You can configure this command globally by using global configuration mode or for a specific interface by using interface configuration mode.

Using this command, you can reset existing values to their default values.

Examples

The following configuration example shows that EAPoUDP parameters have been set to their default values:

```
Router (config)# eou default
```

eou initialize

To manually initialize Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) state machines, use the **eou initialize** command in global configuration mode. This command does not have a **no** form.

eou initialize {**all** | **authentication** {**clientless** | **eap** | **static**} | **interface** *interface-name* | **ip** *ip-address* | **mac** *mac-address* | **posturetoken** *string*}

Syntax Description

all	Initiates reauthentication of all EAPoUDP clients. This keyword is the default.
authentication	Specifies the authentication type.
clientless	Clientless authentication type.
eap	EAP authentication type.
static	Static authentication type.
interface *interface-name*	Specifies a specific interface.
ip *ip-address*	Specifies a specific IP address.
mac *mac-address*	Specifies a specific MAC address.
posturetoken *string*	Specifies a specific posture token.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

If this command is used, existing EAPoUDP state machines will be reset.

Examples

The following example shows that all EAPoUDP state machines have been reauthenticated:

```
Router (config)# eou initialize all
```

Related Commands

Command	Description
eou revalidate	Revalidates an EAPoUDP association.

eou logging

To enable Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) system logging events, use the **eou logging** command in global configuration mode. To remove EAPoUDP logging, use the **no** form of this command.

eou logging

no eou logging

Syntax Description

This command has no arguments or keywords.

Defaults

Logging is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Examples

The following example shows that EAPoUDP logging has been enabled:

```
Router (config)# eou logging
```

The following is sample EAPoUDP logging output:

```
Apr  9 10:04:09.824: %EOU-6-SESSION: IP=10.0.0.1| HOST=DETECTED| Interface=FastEthernet0/0
*Apr  9 10:04:09.900: %EOU-6-CTA: IP=10.0.0.1| CiscoTrustAgent=DETECTED
*Apr  9 10:06:19.576: %EOU-6-POLICY: IP=10.0.0.1| TOKEN=Healthy
*Apr  9 10:06:19.576: %EOU-6-POLICY: IP=10.0.0.1| ACLNAME=#ACSACL#-IP-HealthyACL-40921e54
*Apr  9 10:06:19.576: %EOU-6-POSTURE: IP=10.0.0.1| HOST=AUTHORIZED|
Interface=FastEthernet0/0.420
*Apr  9 10:06:19.580: %EOU-6-AUTHTYPE: IP=10.0.0.1| AuthType=EAP
*Apr  9 10:06:04.424: %EOU-6-SESSION: IP=192.168.2.1| HOST=REMOVED|
Interface=FastEthernet0/0.420
```

eou max-retry

To set the number of maximum retry attempts for Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP), use the **eou max-retry** command in global or interface configuration mode. To remove the number of retries that were entered, use the **no** form of this command.

eou max-retry *number-of-retries*

no eou max-retry *number-of-retries*

Syntax Description

number-of-retries	Number of maximum retries that may be attempted. The value ranges from 1 through 10. The default is 3.

Defaults

The default number of retries is 3.

Command Modes

Global configuration (config)
Interface configuration (config-if)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4	The value range was changed from 1 through 3 to 1 through 10.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

You can configure this command globally by using global configuration mode or for a specific interface by using interface configuration mode.

Examples

The following example shows that the maximum number of retries for an EAPoUDP session has been set for 2:

```
Router (config)# eou max-retry 2
```

Related Commands

Command	Description
show eou	Displays information about EAPoUDP global values or EAPoUDP session cache entries.

eou port

To set the UDP port for Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP), use the **eou port** command in global configuration mode. This command has no **no** form.

eou port *port-number*

Syntax Description

port-number	Number of the port. The value ranges from 1 through 65535. The default value is 27186.

Defaults

The default *port-number* value is 27186.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Ensure that the port you set does not conflict with other UDP applications.

Examples

The following example shows that the port for an EAPoUDP session has been set to 200:

```
Router (config)# eou port 200
```

Related Commands

Command	Description
show eou	Displays information about EAPoUDP.

eou rate-limit

To set the number of simultaneous posture validations for Extensible Authentication Protocol over UDP (EAPoUDP), use the **eou rate-limit** command in global configuration mode. This command has no **no** form.

eou rate-limit *number-of-validations*

Syntax Description

number-of-validations	Number of clients that can be simultaneously validated. The value ranges from 1 through 200. The default value is 20.

Defaults

No default behaviors or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

If you set the rate limit to 0 (zero), rate limiting will be turned off.

If the rate limit is set to 100 and there are 101 clients, validation will not occur until one drops off.

To return to the default value, use the **eou default** command.

Examples

The following example shows that the number of posture validations has been set to 100:

```
Router (config)# eou rate-limit 100
```

Related Commands

Command	Description
eou default	Sets global EAPoUDP parameters to the default values.
show eou	Displays information about EAPoUDP.

eou revalidate

To revalidate an Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) association, use the **eou revalidate** command in privileged EXEC mode. To disable the revalidation, use the **no** form of this command.

eou revalidate {**all** | **authentication** {**clientless** | **eap** | **static**} | **interface** *interface-name* | **ip** *ip-address* | **mac** *mac-address* | **posturetoken** *string*}

no eou revalidate {**all** | **authentication** {**clientless** | **eap** | **static**} | **interface** *interface-name* | **ip** *ip-address* | **mac** *mac-address* | **posturetoken** *string*}

Syntax Description

all	Enables revalidation of all EAPoUDP clients. This keyword option is the default.
authentication	Specifies the authentication type.
clientless	Clientless authentication type.
eap	EAP authentication type.
static	Static authentication type.
interface *interface-name*	Name of the interface. (See Table 33 for the types of interface that may be shown.)
ip *ip-address*	IP address of the client.
mac *mac-address*	The 48-bit hardware address of the client.
posturetoken *string*	Name of the posture token.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

If you use this command, existing EAPoUDP sessions will be revalidated.

Table 33 lists the interface types that may be used with the **interface** keyword.

Table 33 Description of Interface Types

Interface Type	Description
Async	Asynchronous interface
BVI	Bridge-Group Virtual Interface

Table 33 Description of Interface Types (continued)

Interface Type	Description
CDMA-Ix	Code division multiple access Internet exchange (CDMA Ix) interface
CTunnel	Connectionless Network Protocol (CLNS) tunnel (Ctunnel) interface
Dialer	Dialer interface
Ethernet	IEEE 802.3 standard interface
Lex	Lex interface
Loopback	Loopback interface
MFR	Multilink Frame Relay bundle interface
Multilink	Multilink-group interface
Null	Null interface
Serial	Serial interface
Tunnel	Tunnel interface
Vif	Pragmatic General Multicast (PGM) Multicase Host interface
Virtual-PPP	Virtual PPP interface
Virtual-Template	Virtual template interface
Virtual-TokenRing	Virtual TokenRing interface

Examples

The following example shows that all EAPoUDP clients are to be revalidated:

```
Router# eou revalidate all
```

Related Commands

Command	Description
eou initialize	Manually initializes EAPoUDP state machines.

eou timeout

To set the Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) timeout values, use the **eou timeout** command in global or interface configuration mode. To remove the value that was set, use the **no** form of this command.

eou timeout {**aaa** *seconds* | **hold-period** *seconds* | **retransmit** *seconds* | **revalidation** *seconds* | **status query** *seconds*}

no timeout {**aaa** *seconds* | **hold-period** *seconds* | **retransmit** *seconds* | **revalidation** *seconds* | **status query** *seconds*}

Syntax Description

aaa *seconds*	Authentication, authorization, and accounting (AAA) timeout period, in seconds. The value range is from 1 through 60. Default=60.
hold-period *seconds*	Hold period following failed authentication, in seconds. The value range is from 60 through 86400. Default=180.
retransmit *seconds*	Retransmit period, in seconds. The value range is from 1 through 60. Default=3.
revalidation *seconds*	Revalidation period, in seconds. The value range is from 300 through 86400. Default=36000.
status query *seconds*	Status query period after revalidation, in seconds. The value range is from 30 through 1800. Default=300.

Defaults

No default behavior or values

Command Modes

Global configuration (config)
Interface configuration (config-if)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

You can configure this command globally by using global configuration mode or for a specific interface by using interface configuration mode.

Examples

The following example shows that the status query period after revalidation is set to 30:

```
Router (config)# eou timeout status query 30
```

Related Commands

Command	Description
show eou	Displays information about EAPoUDP global values.

error-msg

To display a specific error message when a user logs on to a Secure Sockets Layer Virtual Private Network (SSL VPN) gateway, use the **error-msg** command in webvpn acl configuration mode. To remove the error message, use the **no** form of this command.

error-msg *message-string*

no error-msg *message-string*

Syntax Description

message-string	Error message to be displayed.

Command Default

No special error message is displayed.

Command Modes

Webvpn acl configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

If the **error-url** command is configured, the user is redirected to the error URL for every request that is not allowed. If the **error-url** command is not configured, the user gets a standard, gateway-generated information page showing the message that was configured using the **error-msg** command.

Examples

This example shows that the following error message will be displayed when the user logs on to the SSL VPN gateway:

```
webvpn context context1
 acl acl1
  error-msg "If you have any questions, please contact <a
  href+mailto:employee1@example.com>Employee1</a>."
```

Related Commands

Command	Description
acl	Defines an ACL using a SSL VPN gateway at the Application Layer level and enters webvpn acl configuration mode.
error-url	Defines a URL as an ACL violation page using a SSL VPN gateway.
webvpn context	Configures a SSL VPN context and enters webvpn context configuration mode.

error-url

To define a URL as an access control list (ACL) violation page using a Secure Socket Layer Virtual Private Network (SSL VPN) gateway, use the **error-url** command in webvpn acl configuration mode. To remove the ACL violation page, use the **no** form of this command.

error-url *access-deny-page-url*

no error-url *access-deny-page-url*

Syntax Description

access-deny-page-url	URL to which a user is directed for an ACL violation.

Command Default

If this command is not configured, the gateway redirects the ACL violation page to a predefined URL.

Command Modes

Webvpn acl configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

If the **error-url** command is configured, the user is redirected to a predefined URL for every request that is not allowed. If the **error-url** command is not configured, the user gets a standard, gateway-generated error page.

Examples

The following example shows that the URL “http://www.example.com” has been defined as the ACL violation page:

```
webvpn context context1
 acl acl1
  error-url “http://www.example.com”
```

Related Commands

Command	Description
acl	Defines an ACL using a SSL VPN gateway at the Application Layer level.
error-msg	Displays a specific error message when a user logs on to a SSL VPN gateway.
webvpn context	Configures the SSL VPN context and enters webvpn context configuration mode.

evaluate

To nest a reflexive access list within an access list, use the **evaluate** command in access-list configuration mode. To remove a nested reflexive access list from the access list, use the **no** form of this command.

evaluate *name*

no evaluate *name*

Syntax Description

name	The name of the reflexive access list that you want evaluated for IP traffic entering your internal network. This is the name defined in the **permit** (reflexive) command.

Defaults

Reflexive access lists are not evaluated.

Command Modes

Access-list configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is used to achieve reflexive filtering, a form of session filtering.

Before this command will work, you must define the reflexive access list using the **permit** (reflexive) command.

This command nests a reflexive access list within an extended named IP access list.

If you are configuring reflexive access lists for an external interface, the extended named IP access list should be one which is applied to inbound traffic. If you are configuring reflexive access lists for an internal interface, the extended named IP access list should be one which is applied to outbound traffic. (In other words, use the access list opposite of the one used to define the reflexive access list.)

This command allows IP traffic entering your internal network to be evaluated against the reflexive access list. Use this command as an entry (condition statement) in the IP access list; the entry “points” to the reflexive access list to be evaluated.

As with all access list entries, the order of entries is important. Normally, when a packet is evaluated against entries in an access list, the entries are evaluated in sequential order, and when a match occurs, no more entries are evaluated. With a reflexive access list nested in an extended access list, the extended access list entries are evaluated sequentially up to the nested entry, then the reflexive access list entries are evaluated sequentially, and then the remaining entries in the extended access list are evaluated sequentially. As usual, after a packet matches *any* of these entries, no more entries will be evaluated.

Examples

The following example shows reflexive filtering at an external interface. This example defines an extended named IP access list *inboundfilters*, and applies it to inbound traffic at the interface. The access list definition permits all Border Gateway Protocol and Enhanced Interior Gateway Routing Protocol traffic, denies all Internet Control Message Protocol traffic, and causes all Transmission Control Protocol traffic to be evaluated against the reflexive access list *tcptraffic*.

If the reflexive access list *tcptraffic* has an entry that matches an inbound packet, the packet will be permitted into the network. *tcptraffic* only has entries that permit inbound traffic for existing TCP sessions.

```
interface Serial 1
 description Access to the Internet via this interface
 ip access-group inboundfilters in
!
ip access-list extended inboundfilters
 permit 190 any any
 permit eigrp any any
 deny icmp any any
 evaluate tcptraffic
```

Related Commands

Command	Description
ip access-list	Defines an IP access list by name.
ip reflexive-list timeout	Specifies the length of time that reflexive access list entries will continue to exist when no packets in the session are detected.
permit (reflexive)	Creates a reflexive access list and enables its temporary entries to be automatically generated.

event-action

To change router actions for a signature or signature category, use the **event-action** command in signature-definition-action-engine or IPS-category-action configuration mode. To revert to the default router action values, use the **no** form of this command.

event-action *action*

no event-action

Syntax Description

action	Router actions for a specified signature or signature category. The *action* argument can be any of the following options: • **deny-attacker-inline** • **deny-connection-inline** • **deny-packet-inline** • **produce-alert** • **reset-tcp-connection** **Note** Event actions for an individual signature must be entered on a single line. However, event actions associated with a category can be entered separately or on a single line.

Command Default

Default values for the signature or signature category will be used.

Command Modes

Signature-definition-action-engine configuration (config-sigdef-action-engine)
IPS-category-action configuration (config-ips-category-action)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Signature-Based Changes

After signature-based changes are complete, Cisco IOS Intrusion Prevention System (IPS) prompts the user to confirm whether or not the changes are acceptable. Confirming the changes instructs Cisco IOS IPS to compile the changes for the signature and modify memory structures to reflect the change. Also, Cisco IOS IPS will save the changes to the location specified via the **ip ips config location** command (for example, flash:ips5/*.xml).

You can issue the **show ip ips signatures** command to verify the event-action configuration. (The **show running-config** command does not show individual signature tuning information.)

Signature Category-Based Changes

After signature category-based changes are complete, the category tuning information is saved in the command-line interface (CLI) configuration.

Category configuration information is processed in the order that it is entered. Thus, it is recommended that the process of retiring all signatures occur before all other category tuning.

If a category is configured more than once, the parameters entered in the second configuration will be added to or will replace the previous configuration.

Examples

The following example shows how to configure signature 5726 to reset all TCP connections and produce an alert:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ips signature-definition
Router(config-sigdef)# signature 5726 0
Router(config-sigdef-sig)# engine
Router(config-sigdef-sig-engine)# event-action reset-tcp-connection produce-alert
Router(config-sigdef-sig-engine)# exit
Router(config-sigdef-sig)# exit
Router(config-sigdef)#^ZDo you want to accept these changes? [confirm]
Router#
*Nov 9 21:50:55.847: %IPS-6-ENGINE_BUILDING: multi-string - 3 signatures - 12 of 11
engines
*Nov 9 21:50:55.859: %IPS-6-ENGINE_READY: multi-string - build time 12 ms - packets for
this engine will be scanned
*Nov 9 21:50:55.859: %SYS-5-CONFIG_I: Configured from console by cisco on console
```

The following example shows how to tune event-action parameters for the signature category "adware/spyware." All the tuning information will be applied to all signatures that belong to the adware/spyware signature category.

```
Router(config)# ip ips signature category
Router(config-ips-category)# category attack adware/spyware
Router(config-ips-category-action)# event-action produce-alert
Router(config-ips-category-action)# event-action deny-packet-inline
Router(config-ips-category-action)# event-action reset-tcp-connection
Router(config-ips-category-action)# retired false
Router(config-ips-category-action)# ^Z
Do you want to accept these changes:[confirmm]y
```

Related Commands

Command	Description
engine	Enters the signature-definition-action-engine configuration mode, which allows you to change router actions for a specified signature.
ip ips config location	Specifies the location in which the router will save signature information.
signature	Specifies a signature for which the CLI user tunings will be changed.
show ip ips	Displays IPS information such as configured sessions and signatures.

exclusive-domain

To add or remove a domain name to or from the exclusive domain list so that the Cisco IOS firewall does not have to send lookup requests to the vendor server, use the **exclusive-domain** command in URL parameter-map configuration mode. To disable this capability, use the **no** form of this command.

exclusive-domain {**deny** | **permit**} *domain-name*

no exclusive-domain {**deny** | **permit**} *domain-name*

Syntax Description

deny	Removes the specified domain name from the exclusive domain list. Blocks all traffic destined for the specified domain name.
permit	Adds the specified domain name to the exclusive domain list. Permits all traffic destined for the specified domain name.
domain-name	Domain name that is added or removed from the exclusive domain name list; for example, www.example.com.

Command Default

Disabled.

Command Modes

URL parameter-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

When you are creating or modifying a URL parameter map, you can enter the **exclusive-domain** subcommand after you enter the **parameter-map type urlfilter** command. For detailed information about creating a parameter map, see the **parameter-map type urlfilter** command.

The **exclusive-domain** command allows you to specify a list of domain names (exclusive domains) so that the Cisco IOS firewall does not create a lookup request for the traffic that is destined for one of the domains in the exclusive list. Thus, you can avoid sending lookup requests to the web server for traffic that is destined for a host that is completely allowed to all users. You can enter the complete domain name or a partial domain name.

Complete Domain Name

If you add a complete domain name, such as www.example.com, to the exclusive domain list, all traffic whose URLs are destined for this domain (such as www.example.com/news and www.example.com/index) is excluded from the URL filtering policies of the vendor server. On the basis of the configuration, the URLs are permitted or blocked (denied).

Partial Domain Name

If you add only a partial domain name to the exclusive domain list, such as example.com, all URLs whose domain names end with this partial domain name (such as www.example.com/products and www.example.com/eng) are excluded from the URL filtering policies of the vendor server. On the basis of the configuration, the URLs are permitted or blocked (denied).

Examples

The following example adds cisco.com to the exclusive domain list:

```
parameter-map type urlfilter u1
 exclusive-domain permit example.com
```

Related Commands

Command	Description
ip urlfilter exclusive-domain	Adds or removes a domain name to or from the exclusive domain list so that the Cisco IOS firewall does not have to send lookup requests to the vendor server.
parameter-map type urlfilter	Creates or modifies a parameter map for URL filtering parameters.

filter-hash

To specify the hash for verification and validation of decrypted contents, use the **filter-hash** command in FPM match encryption filter configuration mode.

filter-hash *hash-value*

Syntax Description

hash-value	Hash value obtained from the encrypted traffic classification definition file (eTCDF).

Command Default

No hash value is specified.

Command Modes

FPM match encryption filter configuration (c-map-match-enc-config)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

If you have access to an eTCDF or if you know valid values to configure encrypted Flexible Packet Matching (FPM) filters, you can configure the same eTCDF through the command-line interface instead of using the preferred method of loading the eTCDF on the router. You must create a class map of type access-control using the **class-map type** command, and use the **match encrypted** command to configure the match criteria for the class map on the basis of encrypted FPM filters and enter FPM match encryption filter configuration mode. You can then use the appropriate commands to specify the algorithm, cipher key, cipher value, filter hash, filter ID, and filter version. You can copy the values from the eTCDF by opening the eTCDF in any text editor.

Use the **filter-hash** command to specify the hash for verification and validation of decrypted contents.

Examples

The following example shows how to specify the hash value from the eTCDF file for verification and validation of decrypted contents:

```
Router(config)# class-map type access-control match-all c1
Router(config-cmap)# match encrypted
Router(c-map-match-enc-config)# filter-hash AABBCCDD11223344
Router(c-map-match-enc-config)#
```

Related Commands

Command	Description
class-map type	Creates a class map to be used for matching packets to a specified class.
match encrypted	Configures the match criteria for a class map on the basis of encrypted FPM filters and enters FPM match encryption filter configuration mode.

filter-id

To specify a filter-level ID for encrypted filters, use the **filter-id** command in FPM match encryption filter configuration mode.

filter-id *id-value*

Syntax Description

id-value	Filter-level ID value.

Command Default

No filter ID is specified.

Command Modes

FPM match encryption filter configuration (c-map-match-enc-config)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

If you have access to an encrypted traffic classification definition file (eTCDF) or if you know valid values to configure encrypted Flexible Packet Matching (FPM) filters, you can configure the same eTCDF through the command-line interface instead of using the preferred method of loading the eTCDF on the router. You must create a class map of type access-control using the **class-map type** command, and use the **match encrypted** command to configure the match criteria for the class map on the basis of encrypted FPM filters and enter FPM match encryption filter configuration mode. You can then use the appropriate commands to specify the algorithm, cipher key, cipher value, filter hash, filter ID, and filter version. You can copy the values from the eTCDF by opening the eTCDF in any text editor.

Use the **filter-id** command to specify a filter-level ID for encrypted filters.

Examples

The following example shows how to specify the filter ID value for an encrypted filter:

```
Router(config)# class-map type access-control match-all c1
Router(config-cmap)# match encrypted
Router(c-map-match-enc-config)# filter-id id2
Router(c-map-match-enc-config)#
```

Related Commands

Command	Description
class-map type	Creates a class map to be used for matching packets to a specified class.
match encrypted	Configures the match criteria for a class map on the basis of encrypted FPM filters and enters FPM match encryption filter configuration mode.

filter-version

To specify the filter-level version value for the encrypted filter, use the **filter-version** command in FPM match encryption filter configuration mode.

filter-version *version*

Syntax Description

version	Filter-level version value of the encrypted filter.

Command Default

No filter version is specified.

Command Modes

FPM match encryption filter configuration (c-map-match-enc-config)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

If you have access to an encrypted traffic classification definition file (eTCDF) or if you know valid values to configure encrypted Flexible Packet Matching (FPM) filters, you can configure the same eTCDF through the command-line interface instead of using the preferred method of loading the eTCDF on the router. You must create a class map of type access-control using the **class-map type** command, and use the **match encrypted** command to configure the match criteria for the class map on the basis of encrypted FPM filters and enter FPM match encryption filter configuration mode. You can then use the appropriate commands to specify the algorithm, cipher key, cipher value, filter hash, filter ID, and filter version. You can copy the values from the eTCDF by opening the eTCDF in any text editor.

Use the **filter-version** command to specify the filter-level version value for the encrypted filter.

Examples

The following example shows how to specify the filter version for the encrypted filter:

```
Router(config)# class-map type access-control match-all c1
Router(config-cmap)# match encrypted
Router(c-map-match-enc-config)# filter-version v1
Router(c-map-match-enc-config)#
```

Related Commands

Command	Description
class-map type	Creates a class map to be used for matching packets to a specified class.
match encrypted	Configures the match criteria for a class map on the basis of encrypted FPM filters and enters FPM match encryption filter configuration mode.

firewall

To specify secure virtual LAN (VLAN) groups and to attach them to firewall modules, use the **firewall** command in global configuration mode. To disable the configuration, use the **no** form of this command.

firewall {**autostate** | **module** *number* **vlan-group** *number* | **multiple-vlan-interfaces** | **vlan-group** *number vlan-range*}

no firewall {**autostate** | **module** *number* **vlan-group** *number* | **multiple-vlan-interfaces** | **vlan-group** *number vlan-range*}

Syntax Description

autostate	Enables auto state.
module	Specifies the module number to which a VLAN group is attached.
number	Module number. Valid values are from 1 to 6.
vlan-group	Specifies the secure group to which the VLANs are attached.
number	Group number. The range is from 1 to 65535.
multiple-vlan-interfaces	Enables multiple VLAN interfaces mode for firewall modules.
vlan-range	VLAN range. Valid values are from 2 to 1001 and 1006 to 4094.

Command Default

No secure VLAN groups are attached to firewall modules.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Examples

The following example shows how to configure a VLAN group:

```
Router(config)# firewall vlan-group 34 1-20
```

Related Commands

Command	Description
show firewall vlan-group	Displays secure VLANs attached to a secure group.

fpm package-group

To configure flexible packet matching (fpm) package support, use the **fpm package-group** command in global configuration mode. To disable fpm package support, use the **no** form of this command.

fpm package-group [*fpm-group-name*]

no fpm package-group [*fpm-group-name*]

Syntax Description

fpm-group-name	Specifies the fpm package group name.

Command Default

FPM groups are not configured by default.

Command Modes

Global configuration (config)#

Command History

Release	Modification
15.0(1)M	This command was introduced.

Examples

The following example enables **fpm package-group**:

```
Router(config)# fpm package-group fpm-group-76
```

Related Commands

Command	Description
fpm package-info	Enables fpm package transfer.

fpm package-info

To configure flexible packet matching (fpm) package transfer from an fpm server to a local server, use the **fpm package-info** command in global configuration mode. To disable fpm packet transfer, use the **no** form of this command.

fpm package-info

no fpm package-info

Syntax Description

This command has no keywords or arguments.

Command Default

The command is not configured by default.

Command Modes

Global configuration (config)#

Command History

Release	Modification
15.0(1)M	This command was introduced.

Examples

The following example enables fpm package transfer:

```
Router(config)# fpm package-info
```

Related Commands

Command	Description
fpm package-group	Configures fpm package group support.
show fpm package-group	Displays fpm package matching support configuration details.
show fpm package-info	Displays fpm package transfer configuration details.

fqdn (IKEv2 profile)

To derive the name mangler from the remote identity of type Fully Qualified Domain Name (FQDN), use the **fqdn** command in IKEv2 name mangler configuration mode. To remove the name derived from FQDN, use the **no** form of this command.

fqdn {**all** | **domain** | **hostname**}

no fqdn

Syntax Description

all	Derives the name mangler from the entire FQDN.
domain	Derives the name mangler from the domain name of FQDN.
hostname	Derives the name mangler from the hostname of FQDN.

Command Default

No default behavior or values.

Command Modes

IKEv2 name mangler configuration (config-ikev2-name-mangler)

Command History

Release	Modification
15.1(3)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to derive the name mangler from the remote identity of type FQDN.

Examples

The following example shows how to derive a name for the name mangler from the hostname of FQDN:

```
Router(config)# crypto ikev2 name-mangler mangler2
Router(config-ikev2-name-mangler)# fqdn hostname
```

Related Commands

Command	Description
crypto ikev2 name mangler	Defines a name mangler.

grant auto rollover

To enable automatic granting of certificate reenrollment requests for a Cisco IOS subordinate certificate authority (CA) server or registration authority (RA) mode CA, use the **grant auto rollover command** in certificate server configuration mode. To disable automatic granting of certificate reenrollment requests for a Cisco IOS subordinate or RA-mode CA server, use the **no** form of this command.

grant auto rollover {**ca-cert** | **ra-cert**}

no grant auto rollover {**ca-cert** | **ra-cert**}

Syntax Description

ca-cert	Specifies that auto renewal is enabled for the subordinate CA rollover certificate.
ra-cert	Specifies that auto renewal is enabled for the RA-mode CA rollover certificate.

Command Default

Automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA-mode CA reenrollment requests is not enabled. Reenrollment requests will have to be granted manually.

Command Modes

Certificate server configuration (cs-server).

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

The first time a CA is enabled, a certificate request is sent to its superior CA. This initial request must be granted manually. The **grant auto rollover** command allows subsequent renewal certificate grant requests to be automatically processed by the CA for either a subordinate CA certificate (by designating the **ca-cert** keyword) or an RA-mode CA (by designating the **ra-cert** keyword), thereby eliminating the need for operator intervention.

Examples

The following example shows how the user can enable automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server:

```
Router(cs-server)# grant auto rollover ca-cert
```

Related Commands

Command	Description
auto-rollover	Enables the automated CA certificate rollover functionality.
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.

grant auto trustpoint

To specify the certification authority (CA) trustpoint of another vendor from which the Cisco IOS certificate server will automatically grant certificate enrollment requests, use the **grant auto trustpoint** command in certificate server configuration mode.

grant auto trustpoint *label*

Syntax Description

label	Name of the non-Cisco IOS CA trustpoint.

Defaults

No default behavior or values.

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

After the network administrator for the server configures and authenticates a trustpoint for the CA of another vendor, the **grant auto trustpoint** command is issued to reference the newly created trustpoint and enroll the router with a Cisco IOS CA.

Note The newly created trustpoint can only be used one time (which occurs when the router is enrolled with the Cisco IOS CA). After the initial enrollment is successfully completed, the credential information will be deleted from the enrollment profile.

The Cisco IOS certificate server will automatically grant only the requests from clients who were already enrolled with the CA of another vendor. All other requests must be manually granted—unless the server is set to be in auto grant mode (via the **grant automatic** command).

Caution The **grant automatic** command can be used for testing and building simple networks and should be disabled before the network is accessible by the Internet. However, it is recommended that you do not issue this command if your network is generally accessible.

Examples

The following example shows how to configure a client router and a Cisco IOS certificate server to exchange enrollment requests via a certificate enrollment profile:

```
! Define the trustpoint "msca-root" that points to the non-Cisco IOS CA and enroll and
! authenticate the client with the non-Cisco IOS CA.
```

```
crypto pki trustpoint msca-root
 enrollment mode ra
 enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
 ip-address FastEthernet2/0
 revocation-check crl
!
! Configure trustpoint "cs" for Cisco IOS CA.
crypto pki trustpoint cs
 enrollment profile cs1
 revocation-check crl
!
! Define enrollment profile "cs1," which points to Cisco IOS CA and mention (via the
! enrollment credential command) that "msca-root" is being initially enrolled with the
! Cisco IOS CA.
crypto pki profile enrollment cs1
 enrollment url  http://cs:80
 enrollment credential  msca-root!

! Configure the certificate server, and issue the grant auto trustpoint command to
! instruct the certificate server to accept enrollment request only from clients who are
! already enrolled with trustpoint "msca-root."
crypto pki server cs
 database level minimum
 database url nvram:
 issuer-name CN=cs
 grant auto trustpoint msca-root
!
crypto pki trustpoint cs
 revocation-check crl
rsakeypair cs
!
crypto pki trustpoint msca-root
 enrollment mode ra
 enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
 revocation-check crl
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.

grant none

To specify all certificate requests to be rejected, use the **grant none** command in certificate server configuration mode. To disable automatic rejection of certificate enrollment, use the **no** form of this command.

grant none

no grant none

Syntax Description

This command has no arguments or keywords.

Defaults

Certificate enrollment is manual; that is, authorization is required.

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows how to automatically reject all certificate enrollment requests for the certificate server "myserver":

```
Router#(config) ip http server
Router#(config) crypto pki server myserver
Router#(cs-server) database level minimum
Router#(cs-server)# grant none
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.
grant automatic	Specifies automatic certificate enrollment.

grant ra-auto

To specify that all enrollment requests from a Registration Authority (RA) be granted automatically, use the **grant ra-auto** command in certificate server configuration mode. To disable automatic certificate enrollment, use the **no** form of this command.

grant ra-auto

no grant ra-auto

Syntax Description

This command has no arguments or keywords.

Defaults

Certificate enrollment is manual; that is, authorization is required.

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

When grant ra-auto mode is configured on the issuing certificate server, ensure that the RA mode certificate server is running in manual grant mode so that enrollment requests are authorized individually by the RA.

Note For the **grant ra-auto** command to work, you have to include "cn=ioscs RA" or "ou=ioscs RA" in the subject name of the RA certificate.

Examples

The following output shows that the issuing certificate server is configured to issue a certificate automatically if the request comes from an RA:

```
Router (config)# crypto pki server myserver
Router-ca (cs-server)# grant ra-auto
% This will cause all certificate requests that are already authorized by known RAs to be
automatically granted.

Are you sure you want to do this? [yes/no]:yes
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.

group(firewall)

To enter redundancy application group configuration mode, use the **group** command in redundancy application configuration mode. To remove the group configuration, use the **no** form of this command.

group *id*

no group *id*

Syntax Description

id	Redundancy group ID. Valid values are 1 and 2.

Command Default

No group is configured.

Command Modes

Redundancy application configuration (config-red-app)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following example shows how to configure a redundancy group with group ID 1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)#
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.

group (authentication)

To specify the authentication, authorization, and accounting (AAA) TACACS+ server group to use for preauthentication, use the **group** command in AAA preauthentication configuration mode. To remove the **group** command from your configuration, use the **no** form of this command.

group {**tacacs+** *server-group*}

no group {**tacacs+** *server-group*}

Syntax Description

tacacs+	Uses a TACACS+ server for authentication.
server-group	Name of the server group to use for authentication.

Defaults

No method list is configured.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You must configure the **group** command before you configure any other AAA preauthentication command (**clid**, **ctype**, **dnis**, or **dnis bypass**).

Examples

The following example enables Dialed Number Identification Service (DNIS) preauthentication using the abc123 server group and the password aaa-DNIS:

```
aaa preauth
 group abc123
 dnis password aaa-DNIS
```

Related Commands

Command	Description
aaa preauth	Enters AAA preauthentication mode.
dnis (authentication)	Enables AAA preauthentication using DNIS.

group (IKE policy)

To specify one or more Diffie-Hellman (DH) group identifier(s) for use in an Internet Key Exchange (IKE) policy, which defines a set of parameters to be used during IKE negotiation, use the **group** command in Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode. To reset the DH group identifier to the default value, use the **no** form of this command.

group {**1** | **2** | **5** | **14** | **15** | **16** | **19** | **20** | **24**}

no group

Syntax Description

1	Specifies the 768-bit DH group.
2	Specifies the 1024-bit DH group.
5	Specifies the 1536-bit DH group.
14	Specifies the 2048-bit DH group.
15	Specifies the 3072-bit DH group.
16	Specifies the 4096-bit DH group.
19	Specifies the 256-bit elliptic curve DH (ECDH) group.
20	Specifies the 384-bit ECDH group.
24	Specifies the 2048-bit DH/DSA group.

Command Default

DH group 1

Command Modes

ISAKMP policy configuration (config-isakmp)

Command History

Release	Modification
11.3 T	This command was introduced.
12.1(1.3)T	Support was added for DH group 5.
12.4(4)T	Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.2	Support was added for DH groups 14, 15, and 16 on the Cisco ASR 1000 series routers.
15.1(2)T	This command was modified. The **14**, **15**, **16**, **19**, and **20** keywords were added.

Usage Guidelines

The group chosen must be strong enough (have enough bits) to protect the IPsec keys during negotiation. A generally accepted guideline recommends the use of a 2048-bit group after 2013 (until 2030). Either group 14 or group 24 can be selected to meet this guideline. Even if a longer-lived security method is needed, the use of Elliptic Curve Cryptography is recommended, but group 15 and group 16 can also be considered.

The ISAKMP group and the IPsec perfect forward secrecy (PFS) group should be the same if PFS is used. If PFS is not used, a group is not configured in the IPsec crypto map.

Examples

The following example shows how to configure an IKE policy with the 1024-bit DH group (all other parameters are set to the defaults):

```
Router(config)# crypto isakmp policy 15
Router(config-isakmp) group 2
Router(config-isakmp) exit
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
show crypto isakmp policy	Displays the parameters for each IKE policy.

group (IKEv2 proposal)

To specify one or more Diffie-Hellman (DH) group identifier(s) for use in an Internet Key Exchange Version 2 (IKEv2) proposal, use the **group** command in IKEv2 proposal configuration mode. To reset the DH group identifier to the default value, use the **no** form of this command.

group {**1** | **2** | **5** | **14** | **15** | **16** | **19** | **20** | **24**}

no group

Syntax Description

1	Specifies the 768-bit DH group.
2	Specifies the 1024-bit DH group.
5	Specifies the 1536-bit DH group.
14	Specifies the 2048-bit DH group
15	Specifies the 3072-bit DH group.
16	Specifies the 4096-bit DH group.
19	Specifies the 256-bit elliptic curve DH (ECDH) group.
20	Specifies the 384-bit ECDH group.
24	Specifies the 2048-bit DH/DSA group.

Command Default

DH group 2 and 5 in the IKEv2 proposal.

Command Modes

IKEv2 proposal configuration (config-ikev2-proposal)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(2)T	This command was modified. The **14**, **15**, **16**, **19**, and **20** keywords were added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

The group chosen must be strong enough (have enough bits) to protect the IPsec keys during negotiation. A generally accepted guideline recommends the use of a 2048-bit group after 2013 (until 2030). Either group 14 or group 24 can be selected to meet this guideline. Even if a longer-lived security method is needed, the use of Elliptic Curve Cryptography is recommended, but group 15 and group 16 can also be considered.

Examples

The following example shows how to configure an IKEv2 proposal with the 1024-bit DH group:

```
Router(config)# crypto ikev2 proposal proposal1
Router(config-ikev2-proposal)# group 2
```

```
Router(config-ikev2-proposal)# exit
```

Related Commands

Command	Description
crypto ikev2 proposal	Defines an IKEv2 proposal.
encryption (ikev2 proposal)	Specifies the encryption algorithm in an IKEv2 proposal.
integrity (ikev2 proposal)	Specifies the integrity algorithm in an IKEv2 proposal.
show crypto ikev2 proposal	Displays the algorithms configured in each IKEv2 proposal.

group (local RADIUS server)

To enter user group configuration mode and to configure shared settings for a user group, use the **group** command in local RADIUS server configuration mode. To remove the group configuration from the local RADIUS server, use the **no** form of this command.

group *group-name*

no group *group-name*

Syntax Description

group-name	Name of user group.

Defaults

No default behavior or values

Command Modes

Local RADIUS server configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Examples

The following example shows that shared settings are being configured for group “team1”:

```
group team1
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.

Command	Description
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

group (RADIUS)

To specify the authentication, authorization, and accounting (AAA) RADIUS server group to use for preauthentication, use the **group** command in AAA preauthentication configuration mode. To remove the **group** command from your configuration, use the **no** form of this command.

group *server-group*

no group *server-group*

Syntax Description

server-group	Specifies a AAA RADIUS server group.

Defaults

No default behavior or values.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

You must configure a RADIUS server group with the **aaa group server radius** command in global configuration mode before using the **group** command in AAA preauthentication configuration mode.

You must configure the **group** command before you configure any other AAA preauthentication command (**clid**, **ctype**, **dnis**, or **dnis bypass**).

Examples

The following example shows the creation of a RADIUS server group called “maestro” and then specifies that DNIS preauthentication be performed using this server group:

```
aaa group server radius maestro
 server 10.1.1.1
 server 10.2.2.2
 server 10.3.3.3

aaa preauth
 group maestro
 dnis required
```

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
clid	Preauthenticates calls on the basis of the CLID number.
ctype	Preauthenticates calls on the basis of the call type.

Command	Description
dnis (RADIUS)	Preauthenticates calls on the basis of the DNIS number.
dnis bypass (AAA preauthentication configuration)	Specifies a group of DNIS numbers that will be bypassed for preauthentication.

group-lock

The **group-lock** command attribute is used to check if a user attempting to connect to a group belongs to this group. This attribute is used in conjunction with the extended authentication (Xauth) username. The user name must include the group to which it belongs. The group is then matched against the VPN group name (ID_KEY_ID) that is passed during the Internet Key Exchange (IKE). If the groups do not match, then the client connection is terminated.

To allow the extended authentication (Xauth) username to be entered when preshared key authentication is used with IKE, use the **group-lock** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove the group lock, use the **no** form of this command.

Note Preshared keys are supported only. Certificates are not supported.

group-lock

no group-lock

Syntax Description

This command has no arguments or keywords.

Defaults

Group lock is not configured.

Command Modes

ISAKMP group configuration (config-isakmp-group)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

The Group-Lock attribute can be used if preshared key authentication is used with IKE. When the user enables the **group-lock** command attribute, one of the following extended Xauth usernames can be entered:

name/group

name\group

name@group

name%group

where the \ / @ % are the delimiters. The group that is specified after the delimiter is then compared against the group identifier that is sent during IKE aggressive mode. The groups must match or the connection is rejected.

Caution Do not use the Group-Lock attribute if you are using RSA signature authentication mechanisms such as certificates. Use the User-VPN-Group attribute instead.

The Group-Lock attribute is configured on a Cisco IOS router or in the RADIUS profile. This attribute has local (gateway) significance only and is not passed to the client.

Note If local authentication is used, then the Group-Lock attribute is the only option.

The username in the local or RADIUS database must be of the following format:

username[/,\,%,@]group.

Examples

The following example shows how Group-Lock attribute is configured in the CLI using the **group-lock** command:

Note You must enable the **crypto isakmp client configuration group** command, which specifies group policy information that has to be defined or changed, before enabling the **group-lock** command.

```
crypto isakmp client configuration group cisco
  group-lock
```

The following example shows how an attribute-value (AV) pair for the User-VPN-Group attribute is added in the RADIUS configuration:

Note If RADIUS is used for user authentication, then use the User-VPN-Group attribute instead of the Group-Lock attribute.

```
ipsec:group-lock=1
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto isakmp client configuration group	Specifies the DNS domain to which a group belongs.

hash (ca-trustpoint)

To specify the cryptographic hash function the Cisco IOS client will use for self-signed certificates, use the **hash** command in ca-trustpoint configuration mode. To return to the default cryptographic hash function, use the **no** form of this command.

hash {**md5** | **sha1** | **sha256** | **sha384** | **sha512**}

no hash

Syntax Description

md5	Specifies that Message-Digest algorithm 5 (MD5), the default hash function, will be used.
sha1	Specifies that Secure Hash Algorithm (SHA-1) hash function will be used.
sha256	Specifies that the SHA-256 hash function will be used.
sha384	Specifies that the SHA-384 hash function will be used.
sha512	Specifies that the SHA-512 hash function will be used.

Command Default

By default, for self-signed certificates, the Cisco IOS client uses the MD5 cryptographic hash function.

Command Modes

Ca-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

The **hash** command in ca-trustpoint configuration mode sets the hash function for the signature that the Cisco IOS client will use to sign its self-signed certificates. This hash setting does not specify what kind of signature the certificate authority (CA) will use when it issues a certificate to this client.

Examples

The following example configures the trustpoint “MyTP” and sets the cryptographic hash function to SHA-384:

```
crypto pki trustpoint MyTP
   enrollment url http://MyTP
   ip-address FastEthernet0/0
   revocation-check none
   hash sha384
```

Related Commands

Command	Description
hash (cs-server)	Specifies the cryptographic hash function the Cisco IOS certificate server will use to sign certificates issued by the CA.

hash (cs-server)

To specify the cryptographic hash function the Cisco IOS certificate server will use to sign certificates issued by the certificate authority (CA), use the **hash** command in cs-server configuration mode. To return to the default cryptographic hash function, use the no form of this command.

hash {**md5** | **sha1** | **sha256** | **sha384** | **sha512**}

no hash

Syntax Description

md5	Specifies that the Message-Digest algorithm 5 (MD5), the default hash function, will be used.
sha1	Specifies that the Secure Hash Algorithm (SHA-1) hash function will be used.
sha256	Specifies that the SHA-256 hash function will be used.
sha384	Specifies that the SHA-384 hash function will be used.
sha512	Specifies that the SHA-512 hash function will be used.

Command Default

By default, to sign certificates issued by CA, the Cisco IOS client uses the MD5 cryptographic hash function.

Command Modes

Cs-server configuration (cs-server)

Command History

Release	Modification
12.4(14)XK	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

The **hash** command in cs-server configuration mode sets the hash function for the signature that the Cisco IOS CA will use to sign all of the certificates issued by the server. If the CA is a root CA, it will use the hash function in its own, self-signed certificate.

Examples

The following example configures a certificate server, MyCS, and sets the cryptographic hash function to SHA-512 for the certificate server:

```
crypto pki server MyCS
database level complete
issuer-name CN=company,L=city,C=country
grant auto
hash sha512
lifetime crl 168
```

The following is sample output from the **show crypto ca certificates** command. This output shows that the CA has been configured and that the hash function SHA-512 has been specified.

```
CA Certificate
Status: Available
Certificate Serial Number: 01
Certificate Usage: Signature
Issuer:
cn=company
l=city
c=country
Subject:
cn=company
l=city
c=country
Validity Date:
start date: 01:32:35 GMT Aug 3 2006
end date: 01:32:35 GMT Aug 2 2009
Associated Trustpoints: MyTP
Certificate Subject:
Name: MyCS.cisco.com
IP Address: 192.168.10.2
Status: Pending Key
Usage: General Purpose
Certificate Request Fingerprint SHA1: 05080A60 82DE9395 B35607C2 38F3A0C3 50609EF8
Associated Trustpoint: MyTP
```

Related Commands

Command	Description
hash (ca-trustpoint)	Specifies the cryptographic hash function the Cisco IOS client will use for self-signed certificates.

hash (IKE policy)

To specify the hash algorithm within an Internet Key Exchange policy, use the **hash** command in Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the hash algorithm to the default secure hash algorithm (SHA)-1 hash algorithm, use the **no** form of this command.

hash {**sha** | **sha256** | **sha384** | **md5**}

no hash

Syntax Description

sha	Specifies SHA-1 (HMAC variant) as the hash algorithm.
sha256	Specifies SHA-2 family 256-bit (HMAC variant) as the hash algorithm.
sha384	Specifies SHA-2 family 384-bit (HMAC variant) as the hash algorithm.
md5	Specifies MD5 (HMAC variant) as the hash algorithm.

Defaults

The SHA-1 hash algorithm

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.4(4)T	IPv6 support was added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(2)T	This command was modified. The **sha256** and **sha384** keywords were added.

Usage Guidelines

Use this command to specify the hash algorithm to be used in an IKE policy.

Examples

The following example configures an IKE policy with the MD5 hash algorithm (all other parameters are set to the defaults):

```
crypto isakmp policy 15
 hash md5
 exit
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
group (IKE policy)	Specifies the Diffie-Hellman group identifier within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
show crypto isakmp policy	Displays the parameters for each IKE policy.

heading

To configure the heading that is displayed above URLs listed on the portal page of a SSL VPN, use the **heading** command in webvpn URL list configuration mode. To remove the heading, use the **no** form of this command.

heading *text-string*

no heading

Syntax Description

text-string	The URL list heading entered as a text string. The heading must be in quotation marks if it contains spaces.

Command Default

A heading is not configured.

Command Modes

Webvpn URL list configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

The following example configures a heading for a URL list:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# url-list ACCESS
Router(config-webvpn-url)# heading "Quick Links"
Router(config-webvpn-url)#
```

Related Commands

Command	Description
url-list	Enters webvpn URL list configuration mode to configure the list of URLs to which a user has access on the portal page of a SSL VPN.

hide-url-bar

To prevent the URL bar from being displayed on the SSL VPN portal page, use the **hide-url-bar** command in webvpn group policy configuration mode. To display the URL bar on the portal page, use the **no** form of this command.

hide-url-bar

no hide-url-bar

Syntax Description

This command has no arguments or keywords.

Command Default

The URL bar is displayed on the SSL VPN portal page.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The configuration of this command applies only to clientless mode access.

Examples

The following example hides the URL bar on the SSL VPN portal page:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# hide-url-bar
Router(config-webvpn-group)#
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

host (webvpn url rewrite)

To select the name of the host site to be mangled on a Secure Socket Layer virtual private network (SSL VPN) gateway, use the **host** command in webvpn url rewrite configuration mode. To deselect a site, use the **no** form of this command.

host *host-name*

no host *host-name*

Syntax Description

host-name	Hostname of the site to be mangled.

Command Default

A host site is not selected.

Command Modes

Webvpn url rewrite (config-webvpn-url-rewrite)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example shows that the site www.examplecompany.com is to be mangled:

```
Router (config)# webvpn context
Router (config-webvpn-context)# url rewrite
Router (config-webvpn-url-rewrite)# host www.examplecompany.com
```

Related Commands

Command	Description
ip (webvpn url rewrite)	Configures the IP address of the site to be mangled on an SSL VPN gateway.
unmatched-action (webvpn url rewrite)	Defines the action when the user request does not match the IP address or host site configuration.

hostname (IKEv2 keyring)

To specify the hostname for the peer in the Internet Key Exchange Version 2 (IKEv2) keyring, use the **hostname** command IKEv2 keyring peer configuration mode. To remove the hostname, use the **no** form of this command.

hostname *name*

no hostname

Syntax Description

name	Name for the peer.

Command Default

The hostname is not specified.

Command Modes

IKEv2 keyring peer configuration (config-ikev2-keyring-peer)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

When configuring the IKEv2 keyring, use this command to identify the peer using hostname, which is:

- Independent of the IKEv2 identity.
- Available on an IKEv2 initiator only.
- Provided by IPsec to IKEv2 as part of a security association setup request to identify the peer.
- Used to identify the peer only with crypto maps and not with tunnel protection.

Examples

The following example shows how to configure the hostname for a peer when configuring an IKEv2 keyring:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# description peer1
Router(config-ikev2-keyring-peer)# hostname peer1.example.com
```

Related Commands

Command	Description
address (ikev2 keyring)	Specifies the IPv4 address or the range of the peers in IKEv2 key.
crypto ikev2 keyring	Defines an IKEv2 keyring.

Command	Description
description (ikev2 keyring)	Describes an IKEv2 peer or a peer group for the IKEv2 keyring.
identity (ikev2 keyring)	Identifies the peer with IKEv2 types of identity.
peer	Defines a peer or a peer group for the keyring.
pre-shared-key (ikev2 keyring)	Defines a preshared key for the IKEv2 peer.

hostname (WebVPN)

To configure the hostname for a SSL VPN gateway, use the **hostname** command in webvpn gateway configuration mode. To remove the hostname from the SSL VPN gateway configuration, use the **no** form of this command.

hostname *name*

no hostname

Syntax Description

name	Specifies the hostname.

Command Default

The hostname is not configured.

Command Modes

Webvpn gateway configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

A hostname is configured for use in the URL and cookie-mangling process. In configurations where traffic is balanced among multiple SSL VPN gateways, the hostname configured with this command maps to the gateway IP address configured on the load-balancing device(s).

Examples

The following example configures a hostname for a SSL VPN gateway:

```
Router(config)# webvpn gateway GW_1
Router(config-webvpn-gateway)# hostname VPN_Server
```

Related Commands

Command	Description
webvpn gateway	Defines a SSL VPN gateway and enters webvpn gateway configuration mode.

http proxy-server

To direct Secure Socket Layer virtual private network (SSL VPN) user requests through a backend HTTP proxy server, use the **http proxy-server** command in webvpn policy group configuration mode. To redirect user requests to internal servers, use the **no** form of this command.

http proxy-server {*dns-name* | *ip-address*} **port** *port-number*

no http proxy-server

Syntax Description

dns-name	Domain Name System (DNS) to be directed to the HTTP proxy server.
ip-address	IP address to be directed to the HTTP proxy server.
port *port-number*	Port number of the backend HTTP proxy server.

Command Default

User requests are routed directly to internal servers.

Command Modes

Webvpn policy group configuration (config-webvpn-group)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example shows that requests from IP address 10.1.1.1 are to be routed to the proxy server (port number 2034):

```
Router (config)# webvpn context e1
Router (config-webvpn-context)# policy group g1
Router (config-webvpn-group)# http proxy-server 10.1.1.1 port 2034
Router (config-webvpn-group)# exit
Router (config-webvpn-context)# default-group-policy g1
```

http-redirect

To configure HTTP traffic to be carried over secure HTTP (HTTPS), use the **http-redirect** command in webvpn gateway configuration mode. To remove the HTTPS configuration from the SSL VPN gateway, use the **no** form of this command.

http-redirect [**port** *number*]

no http-redirect

Syntax Description

port *number*	(Optional) Specifies a port number. The value for this argument is a number from 1 to 65535.

Command Default

The following default value is used if this command is configured without entering the **port** keyword:

port *number* : 80

Command Modes

Webvpn gateway configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

When this command is enabled, the HTTP port is opened and the SSL VPN gateway listens for HTTP connections. HTTP connections are redirected to use HTTPS. Entering the **port** keyword and *number* argument configures the gateway to listen for HTTP traffic on the specified port. Entering the **no** form, disables HTTP traffic redirection. HTTP traffic is handled by the HTTP server if one is running.

Examples

The following example, starting in global configuration mode, redirects HTTP traffic (on TCP port 80) over to HTTPS (on TCP port 443):

```
Router(config)# webvpn gateway SSL_GATEWAY
Router(config-webvpn-gateway)# http-redirect
```

Related Commands

Command	Description
webvpn gateway	Defines a SSL VPN gateway and enters webvpn gateway configuration mode.

hw-module slot subslot only

Note This command is deleted effective with Cisco IOS Release 12.2SXI.

To change the mode of the Cisco 7600 SSC-400 card to allocate full buffers to the specified subslot, use the **hw-module slot subslot only** command in global configuration mode. If this command is not used, the total amount of buffers available is divided between the two subslots on the Cisco 7600 SSC-400.

Note This command automatically generates a reset on the Cisco 7600 SSC-400. See Usage Guidelines below for details.

hw-module slot *slot* **subslot** *subslot* **only**

Syntax Description

slot	Chassis slot number where the Cisco 7600 SSC-400 is located. Refer to the appropriate hardware manual for slot information. For SIPs and SSCs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide.
subslot	Secondary slot number on the SSC where the IPSec VPN SPA is installed.

Defaults

No default behavior or values.

Command Modes

Global configuration mode

Command History

Release	Modification
12.2(18)SXF2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2SXI	This command was deleted.

Usage Guidelines

Follow these guidelines and restrictions when configuring a Cisco 7600 SSC-400 and IPSec VPN SPAs using the **hw-module slot subslot only** command:

- This command is useful when supporting IP multicast over GRE on the IPSec VPN SPA.
- When this command is executed, it automatically takes a reset action on the Cisco 7600 SSC-400 and issues the following prompt to the console:

```
Module n will be reset? Confirm [n]:
```

The prompt will default to “N” (no). You must type “Y” (yes) to activate the reset action.

- When in this mode, if you manually plug in a second SPA, or if you attempt to reset the SPA (by entering a **no hw-module subslot shutdown** command, for example), a message is displayed on the router console which refers you to the customer documentation.

Examples

The following example allocates full buffers to the SPA that is installed in subslot 0 of the SIP located in slot 1 of the router and takes a reset action of the Cisco 7600 SSC-400.

```
Router(config)# hw-module slot 4 subslot 1 only
Module 4 will be reset? Confirm [no]: y
```

Note that the prompt will default to “N” (no). You must type “Y” (yes) to activate the reset action.

Related Commands

Command	Description
ip multicast-routing	Enables IP multicast routing.
ip pim	Enables Protocol Independent Multicast (PIM) on an interface.

icmp idle-timeout

To configure the timeout for Internet Control Message Protocol (ICMP) sessions, use the **icmp idle-timeout** command in parameter-map type inspect configuration mode. To disable the timeout, use the **no** form of this command.

icmp idle-timeout *seconds*

no icmp idle-timeout *seconds*

Syntax Description

seconds	ICMP timeout, in seconds. The default is 10.

Command Default

The ICMP timeout is disabled.

Command Modes

Parameter-map type inspect configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

When you are configuring an inspect type parameter map, you can enter the **icmp idle-timeout** subcommand after you enter the **parameter-map type inspect** command. For more detailed information about creating a parameter map, see the **parameter-map type inspect** command.

Examples

The following example specifies that the ICMP session will timeout in 90 seconds:

```
parameter-map type inspect insp-params
 icmp idle-timeout 90
```

Related Commands

Command	Description
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

ida-client server url

To specify the IDA-server url that the IOS IDA client communicates with to download files from the Cisco.com server, use the **ida-client server url** command in global configuration mode. To revert back to the default value, use the **no** form of this command.

ida-client server url *url*

no ida-client server url *url*

Syntax Description

url	Specifies the IDA-server url. You must enter the following URL: https://www.cisco.com/cgi-bin/front.x/ida/locator/locator.pl

Command Default

The default IDA-server URL is: https://www.cisco.com/cgi-bin/ida/locator/locator.pl

Note Do not use the default URL in your configuration.

Command Modes

Global configuration

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.1(1)T	This command was modified to include a default IDA-server URL.

Usage Guidelines

Enter the following URL for the **ida-client server url** command to specify the IDA-server URL:

```
Router(config)# ida-client server url
https://www.cisco.com/cgi-bin/front.x/ida/locator/locator.pl
```

Related Commands

Command	Description
ips signature update cisco	Initiates a one-time download of an IPS signatures from Cisco.com.
upgrade automatic abortversion	Cancels the scheduled reloading of the router with a new Cisco IOS software image.
upgrade automatic getversion	Downloads a Cisco IOS software image directly from www.cisco.com or from a non-Cisco server.
upgrade automatic runversion	Reloads the router with a new Cisco IOS software image.

identity local

To specify the local Internet Key Exchange Version 2 (IKEv2) identity type, use the **identity local** command in IKEv2 profile configuration mode. To remove the identity, use the **no** form of this command.

identity local {**address** {*ipv4-address* | *ipv6-address*} | **dn** | **fqdn** *fqdn-string* | **email** *e-mail-string* | **key-id** *opaque-string*}

no identity local

Syntax Description

address {*ipv4-address* | *ipv6-address*}	Uses the IPv4 or IPv6 address as the local identity.
dn	Uses the distinguished name as the local identity.
fqdn *fqdn-string*	Uses the Fully Qualified Domain Name (FQDN) as the local identity.
email *email-string*	Uses the e-mail ID as the local identity.
key-id *opaque-string*	Uses the proprietary type opaque string as the local identity.

Command Default

If the local authentication method is a preshared key, the default local identity is the IP address (IPv4 or IPv6). If the local authentication method is an RSA signature, the default local identity is Distinguished Name.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. Support was added for IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to specify the local IKEv2 identity type as an IPv4 address or IPv6 address, a DN, an FQDN, an e-mail ID, or a key ID. The local IKEv2 identity is used by the local IKEv2 peer to identify itself to the remote IKEv2 peers in the AUTH exchange using the IDi field.

Note You can configure one local IKEv2 identity type for a profile.

Examples

The following example shows how to specify an IPv4 address as the local IKEv2 identity:

```
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# identity local address 10.0.0.1
```

The following example shows how to specify an IPv6 address as the local IKEv2 identity:

```
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# identity local address 2001:DB8:0::1
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.

identity (IKEv2 keyring)

To identify a peer with Internet Key Exchange Version 2 (IKEv2) types of identity, use the **identity** command in IKEv2 keyring peer configuration mode. To remove the identity, use the **no** form of this command.

identity{**address** {*ipv4-address* | *ipv6-address*} | **fqdn** *name* | **email** *e-mail-id* | **key-id** *key-id*}

no identity

Syntax Description

address {*ipv4-address* | *ipv6-address*}	Uses the IPv4 or IPv6 address to identify the peer.
fqdn *name*	Uses the Fully Qualified Domain Name (FQDN) to identify the peer.
email *e-mail-id*	Uses the e-mail ID to identify the peer.
key-id *key-id*	Uses the proprietory types to identify the peer.

Command Default

Identity types are not specified to a peer.

Command Modes

IKEv2 keyring peer configuration (config-ikev2-keyring-peer)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. Support was added for IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to identify the peer using IKEv2 types of identity such as an IPv4 or IPv6 address, an FQDN, an email, or a key ID. Key lookup using IKEv2 identity is available only on the responder because the peer ID is not available on the initiator at the time of starting the IKEv2 session and the initiator looks up keys during session startup.

Examples

The following example shows how to associate an FQDN to the peer:

```
Router(config)# crypto ikev2 keyring keyring-4
Router(config-keyring)# peer abc
Router(config-keyring-peer)# description abc domain
Router(config-keyring-peer)# identity fqdn example.com
```

Related Commands

Command	Description
address (ikev2 keyring)	Specifies the IPv4 or IPv6 address or the range of the peers in IKEv2 keyring.
crypto ikev2 keyring	Defines an IKEv2 keyring.
description (ikev2 keying)	Describes an IKEv2 peer or a peer group for the IKEv2 keyring.
hostname (ikev2 keyring)	Specifies the hostname for the peer in the IKEv2 keyring.
peer	Defines a peer or a peer group for the keyring.
pre-shared-key (ikev2 keyring)	Defines a preshared key for the IKEv2 peer.

identity (IKEv2 profile)

To specify how the local or remote router identifies itself to the peer and communicates with the peer in the Rivest, Shamir and Adleman (RSA) authentication exchange, use the **identity** command in IKEv2 profile configuration mode. To delete a match, use the **no** form of this command.

identity [**local** {**dn** [**trustpoint** *trustpoint-name* [**serial** *certificate-serial*]] | **address** *ip-address* | **fqdn** *string* | **email** *string*} | **remote** {**dn** [**ou=**..., **o=**...] | **address** *ip-address* | **fqdn** *string* | **email** *string*}]

no identity [**local** {**dn** [**trustpoint** *trustpoint-name* [**serial** *certificate-serial*]] | **address** *ip-address* | **fqdn** *string* | **email** *string*} | **remote** {**dn** [**ou=**..., **o=**...] | **address** *ip-address* | **fqdn** *string* | **email** *string*}]

Syntax Description

local	Specifies the local router.
dn	Specifies the distinguished name (DN) of the local or remote router.
trustpoint *trustpoint-name*	(Optional) Specifies the PKI trustpoint name to use with the RSA signature authentication method on the local router.
serial *certificate-serial*	(Optional) Specifies the serial number of the trustpoint certificate on the local router.
address *ip-address*	Specifies the IP address of the remote or local router.
fqdn *fqdn-name*	Specifies the Fully Qualified Domain Name (FQDN) of the remote or local router.
email *e-mail ID*	Specifies the email ID of the remote or local router.
ou=..., **o=**...	(Optional) Specifies the organizational Unit (OU) field of the subject name in the trustpoint certificate.

Command Default

An identity profile is not specified for a local or remote router regarding the RSA authentication exchange.

Command Modes

IKEv2 profile configuration (crypto-ikev2-profile)#

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(2)T	This command was modified. The **local**, **dn**, **trustpoint**, **serial**, and **ou=** keywords were added to this command.

Usage Guidelines

Use the **identity** command to identify the local or remote router by its DN, trustpoint, IP address, FQDN, or email address.

Examples

The following example shows how an IKEv2 profile is matched on the remote identity. The following profile caters to peers that identify using **fqdn example.com** and authenticate with **rsa-signature** using **trustpoint-remote**. The local node authenticates with **pre-share** using **keyring-1**.

```
Router(config)# crypto ikev2 profile profile2
Router(config-ikev2-profile)# match identity remote fqdn example.com
Router(config-ikev2-profile)# identity local email router2@example.com
Router(config-ikev2-profile)# authentication local pre-share
Router(config-ikev2-profile)# authentication remote rsa-sig
Router(config-ikev2-profile)# keyring keyring-1
Router(config-ikev2-profile)# pki trustpoint trustpoint-remote verify
Router(config-ikev2-profile)# lifetime 300
Router(config-ikev2-profile)# dpd 5 10 on-demand
Router(config-ikev2-profile)# virtual-template 1
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.
match (IKEv2 profile)	Matches a profile on front-door VPN routing and forwarding (FVRF) or local parameters such as IP address or peer identity or peer certificate.
authentication (IKEv2 profile)	Specifies the local and remote authentication methods in an Internet Key Exchange Version 2 (IKEv2) profile.
keyring (IKEv2 profile)	Specifies a locally defined or accounting, authentication and authorization (AAA) based keyring.
pki trustpoint	Specifies the router to use the PKI trustpoints in the RSA signature authentication.

identity address ipv4

To identify a Group Domain of Interpretation (GDOI) group address, use the **identity address ipv4** command in GDOI group configuration mode. To remove the group address, use the **no** form of this command.

identity address ipv4 {*address*}

no identity address ipv4 {*address*}

Syntax Description

address	IP address of the group.

Command Default

A group address is not identified.

Command Modes

GDOI group configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command or the **identity number** command is required for a GDOI configuration.

Examples

The following example shows that the identity address is 10.2.2.2:

```
identity address ipv4 10.2.2.2
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group.
identity number	Identifies a GDOI group number.

identity number

To identify a Group Domain of Interpretation (GDOI) group number, use the **identity number** command in GDOI group configuration mode. To remove the group number, use the **no** form of this command.

identity number {*number*}

no identity number {*number*}

Syntax Description

number	Number of the group.

Command Default

A GDOI group number is not identified.

Command Modes

GDOI group configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command or the **identity address ipv4** command is required for a GDOI configuration.

Examples

The following example shows the group number is 3333:

```
identity number 3333
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
identity address ipv4	Identifies a GDOI group address.

identity policy

To create an identity policy and to enter identity policy configuration mode, use the **identity policy** command in global configuration mode. To remove the policy, use the **no** form of this command.

identity policy *policy-name* [**access-group** *group-name* | **description** *line-of-description* | **redirect** *url* | **template** [**virtual-template** *interface-number*]]

no identity policy *policy-name* [**access-group** *name* | **description** *line-of-description* | **redirect** *url* | **template** [**virtual-template** *interface-number*]]

Syntax Description

policy-name	Name of the policy.
access-group *group-name*	(Optional) Access list to be applied.
description *line-of-description*	(Optional) Description of the policy.
redirect *url*	(Optional) Redirects clients to a particular URL.
template	(Optional) Virtual template interface from which commands may be cloned.
virtual-template *interface-number*	(Optional) Virtual template number. The values range from 1 through 200.

Defaults

An identity policy is not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

An identity policy has to be associated with an identity profile.

Examples

The following example shows that an access policy named “policyname2” is being created. The access-group attribute is set to “allow-access.” The redirect URL is set to “http://remediate-url.com.” This access policy will be associated with a statically authorized device in the identity profile.

```
Router (config)# identity policy policyname2
Router (config-identity-policy)# access-group allow-access
Router (config-identity-policy)# redirect url http://remediate-url.com
```

Related Commands

Command	Description
identity profile	Creates an identity profile.

identity profile

To create an identity profile and to enter identity profile configuration mode, use the **identity profile** command in global configuration mode. To disable an identity profile, use the **no** form of this command.

identity profile {**default** | **dot1x** | **eapoudp** | **auth-proxy**}

no identity profile {**default** | **dot1x** | **eapoudp** | **auth-proxy**}

Syntax Description

default	Service type is default.
dot1x	Service type for 802.1X.
eapoudp	Service type for Extensible Authentication Protocol over UDP (EAPoUDP).
auth-proxy	Service type for authentication proxy.

Command Default

An identity profile is not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(8)T	The **eapoudp** keyword was added.
12.4(6)T	The **dot1x** keyword was removed.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **identity profile** command and **default** keyword allow you to configure static MAC addresses of a client computer that does not support 802.1X and to authorize or unauthorize them statically. After you have issued the **identity profile** command and **default** keyword and the router is in identity profile configuration mode, you can specify the configuration of a template that can be used to create the virtual access interface to which unauthenticated supplicants (client computers) will be mapped.

The **identity profile** command and the **dot1x** keyword are used by the supplicant and authenticator. Using the **dot1x** keyword, you can set the username, password, or other identity-related information for an 802.1X authentication.

Using the **identity profile** command and the **eapoudp** keyword, you can statically authenticate or unauthenticate a device either on the basis of the device IP address or MAC address or on the type, and the corresponding network access policy can be specified using the **identity policy** command.

Examples

The following example shows that an identity profile and its description have been specified:

```
Router (config)# identity profile default
Router (config-identity-prof)# description description_entered_here
```

The following example shows that an EAPoUDP identity profile has been created:

```
Router (config)# identity policy eapoudp
```

Related Commands

Command	Description
debug dot1x	Displays 802.1X debugging information.
description	Specifies a description for an 802.1X profile.
device	Statically authorizes or rejects individual devices.
dot1x initialize	Initializes 802.1X state machines on all 802.1X-enabled interfaces.
dot1x max-req	Sets the maximum number of times that a router can send an EAP request/identity frame to a client PC.
dot1x max-start	Sets the maximum number of times the authenticator sends an EAP request/identity frame (assuming that no response is received) to the client.
dot1x pae	Sets the PAE type during 802.1X authentication.
dot1x port-control	Enables manual control of the authorization state of a controlled port.
dot1x re-authenticate	Manually initiates a reauthtication of the specified 802.1X-enabled ports.
dot1x re-authentication	Globally enables periodic reauthentication of the client PCs on the 802.1X interface.
dot1x system-auth-control	Enables 802.1X SystemAuthControl (port-based authentication).
dot1x timeout	Sets retry timeouts.
identity policy	Creates an identity policy.
show dot1x	Displays details for an identity profile.
template (identity profile)	Specifies a virtual template from which commands may be cloned.

identity profile eapoudp

To create an identity profile and to enter Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) profile configuration mode, use the **identity profile eapoudp** command in global configuration mode. To remove the policy, use the **no** form of this command.

identity profile eapoudp

no identity profile eapoudp

Syntax Description

This command has no arguments or keywords.

Defaults

No EAPoUDP identity profile exists.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Using this command, you can statically authenticate or unauthenticate a device either on the basis of the device IP address or MAC address or on the type, and the corresponding network access policy can be specified using the **identity policy** command.

Examples

The following example shows that an EAPoUDP identity profile has been created:

```
Router (config)# identity profile eapoudp
```

Related Commands

Command	Description
identity policy	Creates an identity policy.

idle-timeout (WebVPN)

Note Effective with Cisco IOS Release 12.4(6)T, the **idle-timeout (WebVPN)** command is not available in Cisco IOS software.

To set the default idle timeout for a Secure Sockets Layer Virtual Private Network (SSLVPN) if no idle timeout has been defined or if the idle timeout is zero (0), use the **idle-timeout** command in Web VPN configuration mode. To revert to the default value, use the **no** form of this command.

idle-timeout [**never** | *seconds*]

no idle-timeout [**never** | *seconds*]

Syntax Description

never	(Optional) The idle timeout function is disabled.
seconds	(Optional) Idle timeout in seconds. The values are from 180 seconds (3 minutes) to 86400 seconds (24 hours).

Defaults

If command is not configured, the default idle timeout is 1800 seconds (30 minutes).

Command Modes

Web VPN configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(6)T	This command was removed.

Usage Guidelines

Configuring this command prevents stale sessions.

Examples

The following example shows that the idle timeout has been set for 1200 seconds:

```
Router (config)# webvpn
Router (config-webvpn)# idle-timeout 1200
```

The following example shows that the idle timeout function is disabled:

```
Router (config)# webvpn
Router (config-webvpn)# idle-timeout never
```

Related Commands

Command	Description
webvpn	Enters Web VPN configuration mode.

if-state nhrp

To enable the Next Hop Resolution Protocol (NHRP) to control the state of the tunnel interface, use the **if-state nhrp** command in interface configuration mode. To disable NHRP control of the tunnel interface state, use the **no** form of this command.

if-state nhrp

no if-state nhrp

Syntax Description

This command has no arguments or keywords.

Command Default

NHRP tunnel interface state control is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

If the system detects that one or more of the Next Hop Servers (NHSs) configured on the interface is up, then the tunnel interface state is also declared as ‘up’. If all NHSs configured on the interface are down, then the tunnel interface state is also declared as ‘down’.

The system does not consider NHSs configured with ‘no-reply’ when determining the interface state.

Examples

The following example shows how to enable NHRP control of the tunnel interface state:

```
Router(config)# interface tunnel 1
Router(config-if)# if-state nhrp
```

Related Commands

Command	Description
show ip interface	Displays the usability status of interfaces configured for IP.
show ip nhrp nhs	Displays NHRP NHS information.

import

To import a user-defined URL list into a webvpn context, use the **import** command in the webvpn URL list configuration mode. To disable the URL list, use the **no** form of this command.

import *device*:*file*

no import *device*:*file*

Syntax Description

device:*file*	• *device*:*file*—Storage device on the system and the file name. The file name should include the directory location.

Command Default

A user-defined URL list is not imported.

Command Modes

Webvpn URL list configuration (config-webvpn-url)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

If this command is used under the **url-list** command, the **url-text** command is not allowed. The **import** command and the **url-list** commands are mutually exclusive when used for a particular URL list. (If you use them together, you will receive this message: "Please remove the imported url-list.")

Also, if a URL list is configured using the **url-text** command, the **import** command is not allowed. (If you use them together, you will receive this message: "Please remove all the URLs before importing a file.")

Examples

The following example shows that the URL list file "test-url.xml" is being imported from flash:

```
Router (config)# webvpn context
 Router (config-webvpn-context)# url-list test
 Router (config-webvpn-url)# import flash:est-url.xml
```

Related Commands

Command	Description
webvpn create template	Creates templates for multilanguage support for messages in an SSL VPN.

include-local-lan

To configure the Include-Local-LAN attribute to allow a nonsplit-tunneling connection to access the local subnetwork at the same time as the client, use the **include-local-lan** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To disable the attribute that allows the nonsplit-tunneling connection, use the **no** form of this command.

include-local-lan

no include-local-lan

Syntax Description

This command has no arguments or keywords.

Defaults

A nonsplit-tunneling connection is not able to access the local subnet at the same time as the client.

Command Modes

ISAKMP group configuration (config-isakmp-group)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

If split tunneling is not in use (that is, the SPLIT_INCLUDE attribute was not negotiated), you lose not only Internet access, but also access to resources on the local subnetworks. The Include-Local-LAN attribute allows the server to push the attribute to the client, which allows for a nonsplit-tunneling connection to access the local subnetwork at the same time as the client (that is, the connection is to the subnetwork to which the client is directly attached).

The Include-Local-LAN attribute is configured on a Cisco IOS router or in the RADIUS profile.

To configure the Include-Local-LAN attribute, use the **include-local-lan** command.

An example of an attribute-value (AV) pair for the Include-Local-LAN attribute is as follows:

```
ipsec:include-local-lan=1
```

You must enable the **crypto isakmp client configuration group** command, which specifies group policy information that has to be defined or changed, before enabling the **include-local-lan** command.

Note

- The Include-Local-LAN attribute can be applied only by a RADIUS user.
- The attribute can be applied on a per-user basis after the user has been authenticated.
- The attribute can override any similar group attributes.

- User-based attributes are available only if RADIUS is used as the database.

Examples

The following example shows that the Include-Local-LAN has been configured:

```
crypto isakmp client configuration group cisco
 include-local-lan
```

Syntax Description

Command	Description
acl	Configures split tunneling.
crypto isakmp client configuration group	Specifies the DNS domain to which a group belongs.

incoming

To configure filtering for incoming IP traffic, use the **incoming** command in router IP traffic export (RITE) configuration mode. To disable filtering for incoming traffic, use the **no** form of this command.

incoming {**access-list** {*standard* | *extended* | *named*} | **sample one-in-every** *packet-number*}

no incoming {**access-list** {*standard* | *extended* | *named*} | **sample one-in-every** *packet-number*}

Syntax Description

access-list {*standard* | *extended* | *named*}	An existing numbered (standard or extended) or named access control list (ACL). **Note** The filter is applied only to exported traffic, not normal router traffic.
sample one-in-every *packet-number*	Exports only one packet out of every specified number of packets. Valid range for the *packet-number* argument is 2 to 2147483647 packets. By default, all traffic is exported.

Defaults

If this command is not enabled, all incoming IP traffic will be filtered via sampling.

Command Modes

RITE configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

When configuring a network device for exporting IP traffic, you can issue the **incoming** command to filter unwanted traffic via the following methods:

- ACLs, which accept or deny an IP packet for export
- Sampling, which allows you to export one in every few packets in which you are interested. Use this option when it is not necessary to export all incoming traffic. Also, sampling is useful when a monitored ingress interface can send traffic faster than the egress interface can transmit it.

Examples

The following example shows how to configure the profile "corp1," which will send captured IP traffic to host "00a.8aab.90a0" at the interface "FastEthernet 0/1." This profile is also configured to export one in every 50 packets and to allow incoming traffic only from the ACL "ham_ACL."

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
```

```
Router(config-if)# ip traffic-export apply corp1
```

Related Commands

Command	Description
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.
outgoing	Configures filtering for outgoing export traffic.

initiate mode

To configure the Phase 1 mode of an Internet Key Exchange (IKE), use the **initiate mode** command in ISAKMP profile configuration mode. To remove the mode that was configured, use the **no** form of this command.

initiate mode aggressive

no initiate mode aggressive

Syntax Description

aggressive	Aggressive mode is initiated.

Defaults

IKE initiates main mode.

Command Modes

ISAKMP profile configuration (config-isa-prof)

Command History

Release	Modification
12.2(15)T	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Use this command if you want to initiate an IKE aggressive mode exchange instead of a main mode exchange.

Examples

The following example shows that aggressive mode has been configured:

```
crypto isakmp profile vpnprofile
 initiate mode aggressive
```

inservice (WebVPN)

To enable a SSL VPN gateway or context process, use the **inservice** command in webvpn gateway configuration or webvpn context configuration mode. To disable a SSL VPN gateway or context process without removing the configuration from the router configuration file, use the **no** form of this command.

inservice

no inservice

Syntax Description

This command has no arguments or keywords.

Command Default

A SSL VPN gateway or context process is not enabled.

Command Modes

Webvpn gateway configuration
Webvpn context configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The enable form of this command initializes required system data structures, initializes TCP sockets, and performs other start-up tasks related to the SSL VPN gateway or context process. The gateway and context processes must both be “inservice” to enable SSL VPN.

Examples

The following example enables the SSL VPN gateway process named SSL_GATEWAY:

```
Router(config)# webvpn gateway SSL_GATEWAY
Router(config-webvpn-gateway)# inservice
```

The following example configures and activates the SSL VPN context configuration:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# inservice
```

Related Commands

Command	Description
webvpn context	Enters webvpn configuration mode to configure the SSL VPN context.
webvpn gateway	Defines a SSL VPN gateway and enters webvpn gateway configuration mode.

inspect

To enable Cisco IOS stateful packet inspection, use the **inspect** command in policy-map-class configuration mode. To disable stateful packet inspection, use the **no** form of this command.

inspect [*parameter-map-name*]

no inspect [*parameter-map-name*]

Syntax Description

parameter-map-name	(Optional) Name of a previously configured inspect parameter-map. If you do not specify a parameter map name, the software uses the default values for all the parameters.

Command Default

None

Command Modes

Policy-map-class configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use this subcommand after entering the **policy-map type inspect**, **class type inspect**, and **parameter-map type** inspect commands.

To enable Cisco IOS stateful packet inspection, enter the name of an inspect parameter-map that was previously configured by using the **parameter-map type inspect** command.

This command lets you specify the attributes that will be used for the inspection.

Examples

The following example specifies inspection parameters for alert and audit-trail, and requests the **inspect** action with the specified parameters:

```
parameter-map type inspect insp-params
 alert on
 audit-trail on

policy-map type inspect mypolicy
 class type inspect inspect-traffic
  inspect inspect-params
```

Related Commands

Command	Description
class type inspect	Specifies the traffic (class) on which an action is to be performed.
parameter-map type inspect	Configures an inspect type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
policy-map type inspect	Creates a Layer 3 or Layer 4 inspect type policy map.

integrity

To specify one or more integrity algorithms for an Internet Key Exchange Version 2 (IKEv2) proposal, use the **integrity** command in IKEv2 proposal configuration mode. To remove the configuration of the hash algorithm, use the **no** form of this command.

integrity {**sha1**} {**sha256**} {**sha384**} {**sha512**} {**md5**}

no integrity

Syntax Description

sha1	Specifies Secure Hash Algorithm (SHA-1 - HMAC variant) as the hash algorithm.
sha256	Specifies SHA-2 family 256-bit (HMAC variant) as the hash algorithm.
sha384	Specifies SHA-2 family 384-bit (HMAC variant) as the hash algorithm.
sha512	Specifies SHA-2 family 512-bit (HMAC variant) as the hash algorithm.
md5	Specifies Message-Digest algorithm 5 (MD5 - HMAC variant) as the hash algorithm.

Command Default

The default integrity algorithm is used.

Command Modes

IKEv2 proposal configuration (config-ikev2-proposal)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(2)T	This command was modified. The **sha256** and **sha384** keywords were added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to specify the integrity algorithm to be used in an IKEv2 proposal. The default integrity algorithms in the default proposal are SHA-1 and MD5.

Note You cannot selectively remove an integrity algorithm when multiple integrity algorithms are configured.

Suite-B adds support for the SHA-2 family (HMAC variant) hash algorithm used to authenticate packet data and verify the integrity verification mechanisms for the IKEv2 proposal configuration. HMAC is a variant that provides an additional level of hashing.

Examples

The following example configures an IKEv2 proposal with the MD5 integrity algorithm:

```
Router(config)# crypto ikev2 proposal proposal1
Router(config-ikev2-proposal)# integrity md5
```

Related Commands

Command	Description
crypto ikev2 proposal	Defines an IKEv2 proposal.
encryption (ikev2 proposal)	Specifies the encryption algorithm in an IKEv2 proposal.
group (ikev2 proposal)	Specifies the Diffie-Hellman group identifier in an IKEv2 proposal.
show crypto ikev2 proposal	Displays the parameters for each IKEv2 proposal.

interface (RITE)

To specify the outgoing interface for exporting traffic, use the **interface** command in router IP traffic export (RITE) configuration mode. To disable an interface, use the **no** form of this command.

interface *interface-name*

no interface *interface-name*

Syntax Description

interface-name	Name of interface in which IP packets are exported.

Defaults

If this command is not enabled, the exported IP traffic profile does not recognize an interface in which to send captured IP traffic.

Command Modes

RITE configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

After you configure an IP traffic export profile via the **ip traffic-export profile** global configuration command, you should issue the **interface** command; otherwise, the profile will be unable to export the captured IP packets. If you do not specify the **interface** command, you will receive a warning, which states that the profile is incomplete, when you attempt to apply the profile to an interface via the **ip traffic-export apply profile** interface configuration command.

Note Currently, only Ethernet and Fast Ethernet interfaces are supported.

Examples

The following example shows how to configure the profile “corp1,” which will send captured IP traffic to host “00a.8aab.90a0” at the interface “FastEthernet 0/1.” This profile is also configured to export one in every 50 packets and to allow incoming traffic only from the access control list ACL “ham_ACL.”

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```

Related Commands

Command	Description
ip traffic-export apply profile	Applies an IP traffic export profile to a specific interface.
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.

interface (VASI)

To configure a Virtual Routing and Forwarding (VRF)-Aware Software Infrastructure (VASI) virtual interface, use the **interface** command in global configuration mode. To remove a VASI configuration, use the **no** form of this command.

interface {**vasileft** | **vasiright**} *number*

no interface {**vasileft** | **vasiright**} *number*

Syntax Description

vasileft	Configures the vasileft interface.
vasiright	Configures the vasiright interface.
number	Identifier of the VASI interface. The range is from 1 to 1000.

Command Default

VASI interface is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.
Cisco IOS XE Release 3.1S	This command was modified. The *number* argument was modified to accept 500 VASI interfaces.
Cisco IOS XE Release 3.3S	This command was modified. The *number* argument was modified to accept 1000 VASI interfaces.

Usage Guidelines

The vasileft and vasiright interfaces must be configured before the VASI interface becomes active. The two halves of the interface pair must be configured separately. If only one half of the interface is configured and not the other half, then the VASI interface does not become active.

Examples

The following example shows how to configure vasileft and vasiright interfaces:

```
Router(config)# interface vasileft 200
router(config-if)# vrf forwarding table1
Router(config-if)# ip address 192.168.0.1 255.255.255.0
Router(config-if)# exit

Router(config)# interface vasiright 200
router(config-if)# vrf forwarding table2
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# exit
```

Related Commands

Command	Description
debug adjacency (VASI)	Displays debugging information for VASI adjacency.
debug interface (VASI)	Displays debugging information for VASI interface descriptor block.
debug vasi	Displays VASI debugging information.
show vasi pair	Displays the status of a VASI pair.

interface virtual-template

To create a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces, use the **interface virtual-template** command in global configuration mode. To remove a virtual template interface, use the **no** form of this command.

interface virtual-template *number*

no interface virtual-template *number*

Syntax Description

number	Number used to identify the virtual template interface. Up to 200 virtual template interfaces can be configured. On the Cisco 10000 series router, up to 4095 virtual template interfaces can be configured.

Command Default

No virtual template interface is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2F	This command was introduced.
12.2(4)T	This command was enhanced to increase the maximum number of virtual template interfaces from 25 to 200.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command's default configuration was modified for SNMP and implemented on the Cisco 10000 series router for the PRE3 and PRE4.

Usage Guidelines

A virtual template interface is used to provide the configuration for dynamically created virtual access interfaces. It is created by users and can be saved in NVRAM.

After the virtual template interface is created, it can be configured in the same way as a serial interface.

Virtual template interfaces can be created and applied by various applications such as virtual profiles, virtual private dialup networks (VPDNs), PPP over ATM, protocol translation, and Multichassis Multilink PPP (MMP).

Cisco 10000 Series Router

You can configure up to 4095 total virtual template interfaces on the Cisco 10000 series router.

To ensure proper scaling and to minimize CPU utilization, we recommend the following virtual template interface settings:

- A keepalive timer of 30 seconds or greater using the **keepalive** command. The default is 10 seconds.

- Do not enable the Cisco Discovery Protocol (CDP). CDP is disabled by default. Use the **no cdp enable** command to disable CDP, if necessary.
- Disable link-status event messaging using the **no logging event link-status** command.
- To prevent the virtual-access subinterfaces from being registered with the SNMP functionality of the router and using memory, do not use the router's SNMP management tools to monitor PPP sessions. Use the **no virtual-template snmp** command to disable the SNMP management tools.

When a virtual template interface is applied dynamically to an incoming user session, a virtual access interface (VAI) is created.

If you configure a virtual template interface with interface-specific commands, the Cisco 10000 series router does not achieve the highest possible scaling. To verify that the router does not have interface-specific commands within the virtual template interface configuration, use the **test virtual-template** <*number*> **subinterface** command.

In Cisco IOS Release 12.2(33)SB, the default configuration for the **virtual-template snmp** command was changed to **no virtual-template snmp**. This prevents large numbers of entries into the MIB ifTable, thereby avoiding CPU Hog messages as SNMP uses the interfaces MIB and other related MIBs. If you configure the **no virtual-template snmp** command, the router no longer accepts the **snmp trap link-status** command under a virtual-template interface. Instead, the router displays a configuration error message such as the following:

```
Router(config)# interface virtual-template 1
Router(config-if)# snmp trap link-status
%Unable set link-status enable/disable for interface
```

If your configuration already has the **snmp trap link-status** command configured under a virtual-template interface and you upgrade to Cisco IOS Release 12.2(33)SB, the configuration error occurs when the router reloads even though the virtual template interface is already registered in the interfaces MIB.

Examples

Cisco 10000 Series Router

The following example creates a virtual template interface called Virtual-Template1:

```
Router(config)# interface Virtual-Template1
Router(config-if)# ip unnumbered Loopback1
Router(config-if)# keepalive 60
Router(config-if)# no peer default ip address
Router(config-if)# ppp authentication pap
Router(config-if)# ppp authorization vpn1
Router(config-if)# ppp accounting vpn1
Router(config-if)# no logging event link-status
Router(config-if)# no virtual-template snmp
```

Virtual Template with PPP Authentication Example

The following example creates and configures virtual template interface 1:

```
interface virtual-template 1 type ethernet
 ip unnumbered ethernet 0
 ppp multilink
 ppp authentication chap
```

IPsec Virtual Template Example

The following example shows how to configure a virtual template for an IPsec virtual tunnel interface.

```
interface virtual-template1 type tunnel
 ip unnumbered Loopback1
```

```
tunnel mode ipsec ipv4
tunnel protection ipsec profile virtualtunnelinterface
```

Related Commands

Command	Description
cdp enable	Enables Cisco Discovery Protocol (CDP) on an interface.
clear interface virtual-access	Tears down the live sessions and frees the memory for other client uses.
keepalive	Enables keepalive packets and to specify the number of times that the Cisco IOS software tries to send keepalive packets without a response before bringing down the interface.
show interface virtual-access	Displays the configuration of the active VAI that was created using a virtual template interface.
tunnel protection	Associates a tunnel interface with an IPsec profile.
virtual interface	Sets the zone name for the connected AppleTalk network.
virtual-profile	Enables virtual profiles.
virtual template	Specifies the destination for a tunnel interface.

ip (webvpn url rewrite)

To configure the IP address of the site to be mangled on a Secure Socket Layer virtual private network (SSL VPN) gateway, use the **ip** command in webvpn url rewrite configuration mode. To deselect the IP address, use the **no** form of this command.

ip *ip-address*

no ip *ip-address*

Syntax Description

ip-address	IP address of the site to be mangled.

Command Default

A site is not selected for mangling.

Command Modes

Webvpn url rewrite (config-webvpn-url-rewrite)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example shows that the IP address 10.1.0.0 255.255.0.0 has been selected for mangling:

```
Router (config)# webvpn context
Router (config-webvpn-context)# url rewrite
Router (config-webvpn-url-rewrite)# ip 10.1.0.0 255.255.0.0
```

Related Commands

Command	Description
host (webvpn url rewrite)	Selects the host name of the site to be mangled on an SSL VPN gateway.
unmatched-action (webvpn url rewrite)	Defines the action when the user request does not match the IP address or host site configuration.

ip access-group

To apply an IP access list or object group access control list (OGACL) to an interface or a service policy map, use the **ip access-group** command in the appropriate configuration mode. To remove an IP access list or OGACL, use the **no** form of this command.

ip access-group {*access-list-name* | *access-list-number*} {**in** | **out**}

no ip access-group {*access-list-number* | *access-list-name*} {**in** | **out**}

Syntax Description

access-list-name	Name of the existing IP access list or OGACL as specified by an **ip access-list** command.
access-list-number	Number of the existing access list. This is a decimal number from 1 to 199 or from 1300 to 2699.
in	Filters on inbound packets.
out	Filters on outbound packets.

Defaults

An access list is not applied.

Command Modes

Interface configuration (config-if)
Service policy-map configuration (config-service-policymap)

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *access-list-name* argument was added.
12.2(28)SB	This command was made available in service policy-map configuration mode.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	The *access-list-name* keyword was modified to accept the name of an OGACL.

Usage Guidelines

If the specified access list does not exist, all packets are passed (no warning message is issued).

Applying Access Lists to Interfaces

Access lists or OGACLs are applied on either outbound or inbound interfaces. For standard inbound access lists, after an interface receives a packet, the Cisco IOS software checks the source address of the packet against the access list. For extended access lists or OGACLs, the networking device also checks the destination access list or OGACL. If the access list or OGACL permits the address, the software continues to process the packet. If the access list or OGACL rejects the address, the software discards the packet and returns an Internet Control Management Protocol (ICMP) host unreachable message.

For standard outbound access lists, after a device receives and routes a packet to a controlled interface, the software checks the source address of the packet against the access list. For extended access lists or OGACLs, the networking device also checks the destination access list or OGACL. If the access list or OGACL permits the address, the software sends the packet. If the access list or OGACL rejects the address, the software discards the packet and returns an ICMP host unreachable message.

When you enable outbound access lists or OGACLs, you automatically disable autonomous switching for that interface. When you enable inbound access lists or OGACLs on any CBus or CxBus interface, you automatically disable autonomous switching for all interfaces (with one exception—a Storage Services Enabler (SSE) configured with simple access lists can still switch packets, on output only).

Applying Access Lists or OGACLs to Service Policy Maps

You can use the **ip access-group** command to configure Intelligent Services Gateway (ISG) per-subscriber firewalls. Per-subscriber firewalls are Cisco IOS IP access lists or OGACLs that are used to prevent subscribers, services, and pass-through traffic from accessing specific IP addresses and ports.

ACLs and OGACLs can be configured in user profiles or service profiles on an authentication, authorization, and accounting (AAA) server or in service policy maps on an ISG. OGACLS or numbered or named IP access lists can be configured on the ISG, or the ACL or OGACL statements can be included in the profile configuration.

When an ACL or OGACL is added to a service, all subscribers of that service are prevented from accessing the specified IP address, subnet mask, and port combinations through the service.

Examples

The following example applies list 101 on packets outbound from Ethernet interface 0:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 0
Router(config-if)# ip access-group 101 out
```

Related Commands

Command	Description
deny	Sets conditions in a named IP access list or OGACL that will deny packets.
ip access-list	Defines an IP access list or OGACL by name or number.
object-group network	Defines network object groups for use in OGACLs.
object-group service	Defines service object groups for use in OGACLs.
permit	Sets conditions in a named IP access list or OGACL that will permit packets.
show ip access-list	Displays the contents of IP access lists or OGACLs.
show object-group	Displays information about object groups that are configured.

ip access-list

To define an IP access list or object-group access control list (ACL) by name or number or to enable filtering for packets with IP helper-address destinations, use the **ip access-list** command in global configuration mode. To remove the IP access list or object-group ACL or to disable filtering for packets with IP helper-address destinations, use the **no** form of this command.

ip access-list {{**standard** | **extended**} {*access-list-name* | *access-list-number*} | **helper egress check**}

no ip access-list {{**standard** | **extended**} {*access-list-name* | *access-list-number*} | **helper egress check**}

Syntax Description

standard	Specifies a standard IP access list.
extended	Specifies an extended IP access list. Required for object-group ACLs.
access-list-name	Name of the IP access list or object-group ACL. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.
access-list-number	Number of the access list. • A standard IP access list is in the ranges 1–99 or 1300–1999. • An extended IP access list is in the ranges 100–199 or 2000–2699.
helper egress check	Enables permit or deny matching capability for an outbound access list that is applied to an interface, for traffic that is relayed via the IP helper feature to a destination server address.

Command Default

No IP access list or object-group ACL is defined, and outbound ACLs do not match and filter IP helper relayed traffic.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was modified. Object-group ACLs are now accepted when the **deny** and **permit** commands are used in standard IP access-list configuration mode or extended IP access-list configuration mode.
Cisco IOS XE Release 3.2S	This command was implemented on Cisco ASR 1000 series routers.
15.0(1)M	This command was modified. The **helper**, **egress**, and **check** keywords were added.

Usage Guidelines

Use this command to configure a named or numbered IP access list or an object-group ACL. This command places the router in access-list configuration mode, where you must define the denied or permitted access conditions by using the **deny** and **permit** commands.

Specifying the **standard** or **extended** keyword with the **ip access-list** command determines the prompt that appears when you enter access-list configuration mode. You must use the **extended** keyword when defining object-group ACLs.

You can create object groups and IP access lists or object-group ACLs independently, which means that you can use object-group names that do not yet exist.

Named access lists are not compatible with Cisco IOS software releases prior to Release 11.2.

Use the **ip access-group** command to apply the access list to an interface.

The **ip access-list helper egress check** command enables outbound ACL matching for permit or deny capability on packets with IP helper-address destinations. When you use an outbound extended ACL with this command, you can permit or deny IP helper relayed traffic based on source or destination User Datagram Protocol (UDP) ports. The **ip access-list helper egress check** command is disabled by default; outbound ACLs will not match and filter IP helper relayed traffic.

Examples

The following example defines a standard access list named Internetfilter:

```
Router> enable
Router# configure terminal
Router(config)# ip access-list standard Internetfilter
Router(config-std-nacl)# permit 192.168.255.0 0.0.0.255
Router(config-std-nacl)# permit 10.88.0.0 0.0.255.255
Router(config-std-nacl)# permit 10.0.0.0 0.255.255.255
```

The following example shows how to create an object-group ACL that permits packets from the users in my_network_object_group if the protocol ports match the ports specified in my_service_object_group:

```
Router> enable
Router# configure terminal
Router(config)# ip access-list extended my_ogacl_policy
Router(config-ext-nacl)# permit tcp object-group my_network_object_group portgroup
my_service_object_group any
Router(config-ext-nacl)# deny tcp any any
```

The following example shows how to enable outbound ACL filtering on packets with helper-address destinations:

```
Router> enable
Router# configure terminal
Router(config)# ip access-list helper egress check
```

Related Commands

Command	Description
deny	Sets conditions in a named IP access list or in an object-group ACL that will deny packets.
ip access-group	Applies an ACL or an object-group ACL to an interface or a service policy map.
object-group network	Defines network object groups for use in object-group ACLs.
object-group service	Defines service object groups for use in object-group ACLs.
permit	Sets conditions in a named IP access list or in an object-group ACL that will permit packets.
show ip access-list	Displays the contents of IP access lists or object-group ACLs.
show object-group	Displays information about object groups that are configured.

ip access-list hardware permit fragments

To permit all noninitial fragments in the hardware, use the **ip access-list hardware permit fragments** command in global configuration mode. To return to the default settings, use the **no** form of this command.

ip access-list hardware permit fragments

no ip access-list hardware permit fragments

Syntax Description

This command has no arguments or keywords.

Defaults

All fragments from flows that are received from an ACE with Layer 4 ports and permit action are permitted. All other fragments are dropped in the hardware. This action also applies to flows that are handled in the software regardless of this command setting.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was changed to affect all ACLs currently applied to interfaces and not just newly-applied ACLs. See the “Usage Guidelines” section for more information.

Usage Guidelines

Flow fragments that match ACEs with Layer 4 ports and permit results are permitted in the hardware, and all other fragments are dropped. An entry is added in the TCAM for each ACE with Layer 4 ports and permit action. This action could cause large ACLs to not fit in the TCAM. If this is the case, use the **ip access-list hardware permit fragments** command to permit all noninitial fragments in the hardware.

Note Configurations that you modify after you entered the **ip access-list hardware permit fragments** command will permit all noninitial fragments in the hardware. Hardware configurations that you modified before you entered the **ip access-list hardware permit fragments** command will not be changed.

Note Hardware configurations that you modify after you entered the **no ip access-list hardware permit fragments** command will return to the default settings. Hardware configurations that you modified before you entered the **no ip access-list hardware permit fragments** command do not change.

The initial flow fragments that match the ACEs with Layer 4 ports and permit results are permitted in the hardware. All other initial fragments are dropped in the hardware.

Catalyst 6500 Series Switches

The following restrictions apply to Cisco IOS releases before Cisco IOS Release 12.2(18)SX5:

Note Configurations that you modify after you entered the **ip access-list hardware permit fragments** command will permit all noninitial fragments in the hardware. Hardware configurations that you modified before you entered the **ip access-list hardware permit fragments** command will not be changed.

Note Hardware configurations that you modify after you entered the **no ip access-list hardware permit fragments** command will return to the default settings. Hardware configurations that you modified before you entered the **no ip access-list hardware permit fragments** command do not change.

In Cisco IOS releases after Cisco IOS Release 12.2(18)SX5, this command affects all ACLs currently applied to interfaces and not just newly-applied ACLs.

Examples

This example shows how to permit all noninitial fragments in the hardware:

```
Router(config)# ip access-list hardware permit fragments
```

This example shows how to return to the default settings:

```
Router(config)# no ip access-list hardware permit fragments
```

Related Commands

Command	Description
show ip interface	Displays the usability status of interfaces that are configured for IP.

ip access-list logging interval

To configure the logging interval for access list entries, use the **ip access-list logging interval** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ip access-list logging interval *interval*

no ip access-list logging interval

Syntax Description

interval	Access list logging interval, in milliseconds. The range is from 0 to 2147483647.

Command Default

Access list logging intervals are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows how to set the access list logging interval to 100 milliseconds:

```
Router# configure terminal
Router(config)# ip access-list logging interval 100
```

Related Commands

Command	Description
ip access-list logging hash-generation	Enables hash-value generation for ACE syslog entries.

ip access-list log-update

To set the threshold number of packets that generate a log message if they match an access list, use the **ip access-list log-update** command in global configuration mode. To remove the threshold, use the **no** form of this command.

ip access-list log-update threshold *number-of-matches*

no ip access-list log-update

Syntax Description

number-of-matches	Threshold number of packets necessary to match an access list before a log message is generated. The range is 0 to 2147483647. There is no default number of matches.

Defaults

Log messages are sent at the first matching packet and at 5-minute intervals after that.

Command Modes

Global configuration

Command History

Release	Modification
12.0(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Log messages are generated if you have specified the **log** keyword in the **access-list (IP standard)**, **access-list (IP extended)**, **deny (IP)**, **dynamic**, or **permit** command.

Log messages provide information about the packets that are permitted or denied by an access list. By default, log messages appear at the console. (The level of messages logged to the console is controlled by the **logging console** command.) The log message includes the access list number, whether the packet was permitted or denied, and other information.

By default, the log messages are sent at the first matching packet and after that, identical messages are accumulated for 5-minute intervals, with a single message being sent with the number of packets permitted and denied during that interval. However, you can use the **ip access-list log-update** command to set the number of packets that, when match an access list (and are permitted or denied), cause the system to generate a log message. You might want to do this to receive log messages more frequently than at 5-minute intervals.

Caution If you set the *number-of-matches* argument to 1, a log message is sent right away, rather than caching it; every packet that matches an access list causes a log message. A setting of 1 is not recommended because the volume of log messages could overwhelm the system.

Even if you use the **ip access-list log-update** command, the 5-minute timer remains in effect, so the cache is emptied at the end of 5 minutes, regardless of the count of messages in the cache. Regardless of when the log message is sent, the cache is flushed and the count reset to 0 for that message the same way it is when a threshold is not specified.

If the syslog server is not directly connected to a LAN that the router shares, any intermediate router might drop the log messages because they are UDP (unreliable) messages.

Examples

The following example enables logging whenever the 1000th packet matches an access list entry:

```
ip access-list log-update threshold 1000
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
deny (IP)	Sets conditions under which a packet is denied by a named IP access list.
dynamic	Defines a named dynamic IP access list.
logging console	Limits messages logged to the console, based on severity.
permit	Sets conditions under which a packet passes a named IP access list.

ip access-list resequence

To apply sequence numbers to the access list entries in an access list, use the **ip access-list resequence** command in global configuration mode.

ip access-list resequence *access-list-name starting-sequence-number increment*

Syntax Description

access-list-name	Name of the access list. Names cannot contain a space or quotation mark.
starting-sequence-number	Access list entries will be resequenced using this initial value. The default value is 10. The range of possible sequence numbers is 1 through 2147483647.
increment	The number by which the sequence numbers change. The default value is 10. For example, if the increment value is 5 and the beginning sequence number is 20, the subsequent sequence numbers are 25, 30, 35, 40, and so on.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command allows the **permit** and **deny** entries of a specified access list to be resequenced with an initial sequence number value determined by the *starting-sequence-number* argument, and continuing in increments determined by the *increment* argument. If the highest sequence number exceeds the maximum possible sequence number, then no sequencing occurs.

For backward compatibility with previous releases, if entries with no sequence numbers are applied, the first entry is assigned a sequence number of 10, and successive entries are incremented by 10. The maximum sequence number is 2147483647. If the generated sequence number exceeds this maximum number, the following message is displayed:

```
Exceeded maximum sequence number.
```

If the user enters an entry without a sequence number, it is assigned a sequence number that is 10 greater than the last sequence number in that access list and is placed at the end of the list.

If the user enters an entry that matches an already existing entry (except for the sequence number), then no changes are made.

If the user enters a sequence number that is already present, the following error message is generated:

```
Duplicate sequence number.
```

If a new access list is entered from global configuration mode, then sequence numbers for that access list are generated automatically.

Distributed support is provided so that the sequence numbers of entries in the Route Processor (RP) and line card (LC) are in synchronization at all times.

Sequence numbers are not saved in NVRAM. That is, the sequence numbers themselves are not saved. In the event that the system is reloaded, the configured sequence numbers revert to the default sequence starting number and increment.

This command works with named standard and extended IP access lists. Because the name of an access list can be designated as a number, numbers are acceptable as names as long as they are entered in named access list configuration mode.

Examples

The following example resequences an access list named kmd1. The starting sequence number is 100, and the increment value is 5:

```
ip access-list resequence kmd1 100 5
```

Related Commands

Command	Description
deny (IP)	Sets conditions under which a packet does not pass a named IP access list.
permit (IP)	Sets conditions under which a packet passes a named IP access list.

ip access-list logging hash-generation

To enable hash-value generation for access control entry (ACE) syslog entries, use the **ip access-list logging hash-generation** command in global configuration mode. To disable hash value generation, use the **no** form of this command.

ip access-list logging hash-generation

no ip access-list logging hash-generation

Syntax Description

This command has no arguments or keywords.

Command Default

Hash value generation is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

Cisco IOS routers generate syslog entries for log-enabled ACEs. The system appends a tag (either a user-defined cookie or a router-generated MD5 hash value) to ACE syslog entries. This tag uniquely identifies the ACE, within an access control list (ACL), that generated the syslog entry.

Use this command to generate an MD5 hash value for all the log enabled ACEs in the system that do not have a user-defined cookie. The system attaches the router-generated hash value to the corresponding ACE. The hash value is stored locally in the router's NVRAM and persists through router reloads.

Examples

The following example shows how to enable hash value generation on the router, for IP access list syslog entries:

```
Router(config)# ip access-list logging hash-generation
Router(config)#
*Aug 7 01:10:12.077: %IPACL-HASHGEN: ACL: 101 seq no : 20 Hash code is 0x75F079
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
debug ip access-list hash-generation	Displays debugging information about ACL hash generation.
show ip access-list	Displays the contents of all current access lists.

ip-address (ca-trustpoint)

To specify a dotted IP address or an interface that will be included as "unstructuredAddress" in the certificate request, use the **ip-address** command in ca-trustpoint configuration mode. To restore the default behavior, use the **no** form of this command.

ip-address {*ip-address* | *interface* | **none**]

no ip-address

Syntax Description

ip-address	Specifies a dotted IP address that will be included as "unstructuredAddress" in the certificate request.
interface	Specifies an interface, from which the router can get an IP address, that will be included as "unstructuredAddress" in the certificate request.
none	Specifies that an IP address is not to be included in the certificate request.

Defaults

An IP address is not configured. You will be prompted for the IP address during certificate enrollment.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Before you can issue this command, you must enable the **crypto ca | pki trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode. The **ip-address** command is a subcommand that allows you to specify a certificate enrollment parameter.

Use the **ip-address** command to include the IP address of the specified interface in the certificate request or to specify that an IP address should not be included in the certificate request.

If this command is enabled, you will not be prompted for an IP address during certificate enrollment.

Examples

The following example shows how to include the IP address of the Ethernet-0 interface in the certificate request for the trustpoint "frog":

```
crypto ca trustpoint frog
 enrollment url http://frog.phoobin.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet-0
```

The following example shows that an IP address is not to be included in the certificate request:

```
crypto ca trustpoint root
 enrollment url http://10.3.0.7:80
 fqdn none
```

```
ip-address none
subject-name CN=subject1, OU=PKI, O=Cisco Systems, C=US
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

ip address dhcp

To acquire an IP address on an interface from the DHCP, use the **ip address dhcp** command in interface configuration mode. To remove any address that was acquired, use the **no** form of this command.

ip address dhcp [**client-id** *interface-type number*] [**hostname** *hostname*]

no ip address dhcp [**client-id** *interface-type number*] [**hostname** *hostname*]

Syntax Description

client-id	(Optional) Specifies the client identifier. By default, the client identifier is an ASCII value. The **client-id** *interface-type number* option sets the client identifier to the hexadecimal MAC address of the named interface.
interface-type	(Optional) Interface type. For more information, use the question mark (?) online help function.
number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
hostname	(Optional) Specifies the hostname.
hostname	(Optional) Name of the host to be placed in the DHCP option 12 field. This name need not be the same as the hostname entered in global configuration mode.

Defaults

The hostname is the globally configured hostname of the router.
The client identifier is an ASCII value.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.1(3)T	This command was modified. The **client-id** keyword and *interface-type number* argument were added.
12.2(3)	This command was modified. The **hostname** keyword and *hostname* argument were added. The behavior of the **client-id** *interface-type number* option changed. See the “Usage Guidelines” section for details.
12.2(8)T	This command was modified. The command was expanded for use on PPP over ATM (PPPoA) interfaces and certain ATM interfaces.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)T	This command was modified. Support was provided on the tunnel interface.

Usage Guidelines

Note Prior to Cisco IOS Release 12.2(8)T, the **ip address dhcp** command could be used only on Ethernet interfaces.

The **ip address dhcp** command allows any interface to dynamically learn its IP address by using the DHCP protocol. It is especially useful on Ethernet interfaces that dynamically connect to an Internet service provider (ISP). Once assigned a dynamic address, the interface can be used with the Port Address Translation (PAT) of Cisco IOS Network Address Translation (NAT) to provide Internet access to a privately addressed network attached to the router.

The **ip address dhcp** command also works with ATM point-to-point interfaces and will accept any encapsulation type. However, for ATM multipoint interfaces you must specify Inverse ARP via the **protocol ip inarp** interface configuration command and use only the aa15snap encapsulation type.

Some ISPs require that the DHCPDISCOVER message have a specific hostname and client identifier that is the MAC address of the interface. The most typical usage of the **ip address dhcp client-id** *interface-type number* **hostname** *hostname* command is when *interface-type* is the Ethernet interface where the command is configured and *interface-type number* is the hostname provided by the ISP.

A client identifier (DHCP option 61) can be a hexadecimal or an ASCII value. By default, the client identifier is an ASCII value. The **client-id** *interface-type number* option overrides the default and forces the use of the hexadecimal MAC address of the named interface.

Note Between Cisco IOS Releases 12.1(3)T and 12.2(3), the **client-id** optional keyword allows the change of the fixed ASCII value for the client identifier. After Release 12.2(3), the optional **client-id** keyword forces the use of the hexadecimal MAC address of the named interface as the client identifier.

If a Cisco router is configured to obtain its IP address from a DHCP server, it sends a DHCPDISCOVER message to provide information about itself to the DHCP server on the network.

If you use the **ip address dhcp** command with or without any of the optional keywords, the DHCP option 12 field (hostname option) is included in the DISCOVER message. By default, the hostname specified in option 12 will be the globally configured hostname of the router. However, you can use the **ip address dhcp hostname** *hostname* command to place a different name in the DHCP option 12 field than the globally configured hostname of the router.

The **no ip address dhcp** command removes any IP address that was acquired, thus sending a DHCPRELEASE message.

You might need to experiment with different configurations to determine the one required by your DHCP server. Table 34 shows the possible configuration methods and the information placed in the DISCOVER message for each method.

Table 34 Configuration Method and Resulting Contents of the DISCOVER Message

Configuration Method	Contents of DISCOVER Messages
ip address dhcp	The DISCOVER message contains "cisco- *mac-address* -Eth1" in the client ID field. The *mac-address* is the MAC address of the Ethernet 1 interface and contains the default hostname of the router in the option 12 field.
ip address dhcp hostname *hostname*	The DISCOVER message contains "cisco- *mac-address* -Eth1" in the client ID field. The *mac-address* is the MAC address of the Ethernet 1 interface, and contains *hostname* in the option 12 field.
ip address dhcp client-id ethernet 1	The DISCOVER message contains the MAC address of the Ethernet 1 interface in the client ID field and contains the default hostname of the router in the option 12 field.
ip address dhcp client-id ethernet 1 hostname *hostname*	The DISCOVER message contains the MAC address of the Ethernet 1 interface in the client ID field and contains *hostname* in the option 12 field.

Examples

In the examples that follow, the command **ip address dhcp** is entered for Ethernet interface 1. The DISCOVER message sent by a router configured as shown in the following example would contain "cisco- *mac-address* -Eth1" in the client-ID field, and the value abc in the option 12 field.

```
hostname abc
!
interface Ethernet 1
 ip address dhcp
```

The DISCOVER message sent by a router configured as shown in the following example would contain "cisco- mac-address -Eth1" in the client-ID field, and the value def in the option 12 field.

```
hostname abc
!
interface Ethernet 1
 ip address dhcp hostname def
```

The DISCOVER message sent by a router configured as shown in the following example would contain the MAC address of Ethernet interface 1 in the client-id field, and the value abc in the option 12 field.

```
hostname abc
!
interface Ethernet 1
 ip address dhcp client-id Ethernet 1
```

The DISCOVER message sent by a router configured as shown in the following example would contain the MAC address of Ethernet interface 1 in the client-id field, and the value def in the option 12 field.

```
hostname abc
!
interface Ethernet 1
 ip address dhcp client-id Ethernet 1 hostname def
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

ip address (WebVPN)

To configure a proxy IP address on a Secure Socket Layer virtual private network (SSL VPN) gateway, use the **ip address** command in webvpn gateway configuration mode. To remove the proxy IP address from the SSL VPN gateway, use the **no** form of this command.

ip address *ip-address* [**port** *port-number*] [**standby** *name*]

no ip address

Syntax Description

ip-address	IPv4 address.
port *port-number*	(Optional) Specifies the port number for proxy traffic. A number from 1 to 65535 can be entered for this argument. The default port number 443 is used if this command is configured without entering the **port** keyword.
standby *name*	• (Optional) Indicates that the IP address is a virtual address configured on one of the router interfaces using Hot StandbyRouting Protocol (HSRP). • *name*—Must be the same as the HSRP group name that was configured on the router interface. **Note** Note that the *name* argument is not an optional parameter when the **standby** keyword is used.

Command Default

A proxy IP address is not configured.

Command Modes

Webvpn gateway configuration (config-webvpn-gateway)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(20)T	The **standby** keyword and *name* arguments were added.

Usage Guidelines

The **ip address** command is used to configure a proxy IP address for an SSL VPN gateway. The IP address is the termination point for all SSL VPN client connections. This IP address can be any routable IP address assigned to a valid interface.

Examples

The following example configures 192.168.1.1 as a proxy address on an SSL VPN gateway. Proxy traffic is directed over port 443.

```
Router(config)# webvpn gateway SSL_GATEWAY
Router(config-webvpn-gateway)# ip address 192.168.1.1 port 443
```

The following example shows that Router 1 and Router 2 are configured for HSRP on Gateway Webvpn:

Router 1 Configuration

```
Router# configure terminal
Router config)# interface g0/1
Router (config-if)# standby 0 ip 10.1.1.1
Router (config-if)# standby 0 name SSLVPN
Router (config-if)# exit
Router (config)# webvpn gateway Webvpn
Router (config-webvpn-gateway)# ip address 10.1.1.1 port 443 standby SSLVPN
```

Router 2 Configuration

```
Router# configure terminal
Router (config)# interface g0/0
Router (config-if)# standby 0 ip 10.1.1.1
Router (config-if)# standby 0 name SSLVPN2
Router (config-if)# exit
Router (config)# webvpn gateway Webvpn
Router (config-webvpn-gateway)# ip address 10.1.1.1 port 443 standby SSLVPN2
```

Related Commands

Command	Description
standby name	Configures the name of the standby group.
webvpn gateway	Defines an SSL VPN gateway and enters webvpn gateway configuration mode.

ip admission

To create a Layer 3 network admission control rule to be applied to the interface, or to create a policy that can be applied on an interface when the authentication, authorization and accounting (AAA) server is unreachable, use the **ip admission** command in interface configuration mode. To create a global policy that can be applied on a network access device, use the **ip admission** command with the optional keywords and argument in global configuration mode. To remove the admission control rule, use the **no** form of this command.

ip admission *admission-name* [**event timeout aaa policy identity** *identity-policy-name*]

no ip admission *admission-name* [**event timeout aaa policy identity** *identity-policy-name*]

Syntax Description

admission-name	Authentication or admission rule name.
event timeout aaa policy identity	Specifies an authentication policy to be applied when the AAA server is unreachable.
identity-policy-name	Authentication or admission rule name to be applied when the AAA server is unreachable.

Command Default

A network admission control rule is not applied to the interface.

Command Modes

Interface configuration (config-if)
Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(11)T	This command was modified to include the **event timeout aaa policy identity** keywords and the *identity-policy-name* argument.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

The admission rule defines how you apply admission control.

The optional keywords and argument define the network admission policy to be applied to a network access device or an interface when no AAA server is reachable. The command can be used to associate a default identity policy with Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) sessions.

Examples

The following example shows how to apply a network admission control rule named “nacrule1” to the interface:

```
Router (config-if)# ip admission nacrule1
```

The following example shows how to apply an identity policy named “example” to the device when the AAA server is unreachable:

```
Router (config)# ip admission nacrule1 event timeout aaa policy identity example
```

Related Commands

Command	Description
interface	Defines an interface.

ip admission consent banner

To display a banner on the authentication proxy consent webpage, use the **ip admission consent banner** command in global configuration mode. To disable a display of the banner, use the **no** form of this command.

ip admission consent banner {**file** *file-name* | **text** *banner-text*}

no ip admission consent banner

Syntax Description

file *file-name*	Specifies a file that is to be shown as the consent webpage.
text *banner-text*	Specifies a text string to replace the default banner, which is the name of the router. The text string should be written in the following format: "C *banner-text* C," where "C" is a delimiting character.

Command Default

A banner is not displayed on the authentication proxy consent webpage.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

The **ip admission consent banner** command allows users to configure one of two possible scenarios:

- The **ip admission consent banner** command with a filename is enabled.

  In this scenario, the administrator supplies the location and name of the file that is to be used for the consent webpage.

- The **ip admission consent banner** command with the banner text is enabled.

  In this scenario, the administrator can supply multiline text that will be converted to HTML by the auth-proxy parser code. Thus, only the multiline text is displayed on the authentication proxy login page.

Note If the **ip admission consent banner** command is not enabled, nothing will be displayed to the user on a consent login page except a text box to enter the username and a text box to enter the password.

Note When HTTP authentication proxy is configured together with the Consent feature, any HTTP authentication proxy-related configurations or policies will override the Consent Page-related configurations or policies. For example, if the **ip admission name** *admission-name* **consent** command is configured, the **ip admission consent banner** command is ignored, and only the banner that is configured by the **ip admission auth-proxy-banner** command is shown.

Examples

The following example shows how to display the file “consent_page.html” located in flash:

```
ip admission consent-banner file flash:consent_page.html
```

The following example shows how to specify the custom banner “Consent-Page-Banner-Text” to be displayed in the authentication proxy consent webpage:

```
ip admission consent-banner text ^C Consent-Page-Banner-Text ^C
```

Related Commands

Command	Description
ip auth-proxy auth-proxy-banner	Displays a banner, such as the router name, in the authentication proxy login page.

ip admission name

To create an IP network admission control rule, use the **ip admission name** command in global configuration mode. To remove the network admission control rule, use the **no** form of this command.

ip admission name *admission-name* [**eapoudp** [**bypass**] | **proxy** {**ftp** | **http** | **telnet**} | **service-policy type tag** {*service-policy-name*}] [**list** {*acl* | *acl-name*}] [**event**] [**timeout aaa**] [**policy identity** {*identity-policy-name*}]

no ip admission name *admission-name* [**eapoudp** [**bypass**] | **proxy** {**ftp** | **http** | **telnet**} | **service-policy type tag** {*service-policy-name*}] [**list** {*acl* | *acl-name*}] [**event**] [**timeout aaa**] [**policy identity** {*identity-policy-name*}]

Syntax for Authentication Proxy Consent Webpage

ip admission name *admission-name* **consent** [[**absolute-timer** *minutes*] [**event**] [**inactivity-time** *minutes*] [**list** {*acl* | *acl-name*}] [**parameter-map** *consent-parameter-map-name*]]

no ip admission name *admission-name* **consent** [[**absolute-timer** *minutes*] [**event**] [**inactivity-time** *minutes*] [**list** {*acl* | *acl-name*}] [**parameter-map** *consent-parameter-map-name*]]

Syntax Description

admission-name	Name of network admission control rule.
eapoudp	(Optional) Specifies IP network admission control using Extensible Authentication Protocol over UDP (EAPoUDP).
bypass	(Optional) Admission rule bypasses EAPoUDP communication.
proxy	(Optional) Specifies authentication proxy.
ftp	Specifies that FTP is to be used to trigger the authentication proxy.
http	Specifies that HTTP is to be used to trigger authentication proxy.
telnet	Specified that Telnet is to be used to trigger authentication proxy.
service-policy type tag	(Optional) A control plane service policy is to be configured.
service-policy-name	Control plane tag service policy that is configured using the **policy-map type control tag** {*policy name*} command, keyword, and argument. This policy map is used to apply the actions on the host when a tag is received.
list	(Optional) Associates the named rule with an access control list (ACL).
acl	Applies a standard, extended list to a named admission control rule. The value ranges from 1 through 199.
acl-name	Applies a named access list to a named admission control rule.
event	(Optional) Identifies the condition that triggered the application of the policy.
timeout aaa	(Optional) Specifies that the AAA server is unreachable.
policy identity	Configures the application of an identity policy to be used while the AAA server is unreachable.
identity-policy-name	Specifies the identity policy to apply.

consent	Associates an authentication proxy consent webpage with the IP admission rule specified via the *admission-name* argument.
absolute-timer *minutes*	(Optional) Elapsed time, in minutes, before the external server times out.
inactivity-time *minutes*	(Optional) Elapsed time, in minutes, before the external file server is deemed unreachable.
parameter-map	(Optional) A parameter map policy is to be associated with consent profile.
consent-parameter-map-name	Specifies the consent profile parameters to apply.

Command Default

An IP network admission control rule is not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(6)T	The **bypass** and **service-policy type tag** keywords and *service-policy-name* argument were added.
12.4(11)T	The **event**, **timeout aaa**, and **policy identity** keywords and the *identity-policy-name* argument were added.
12.4(15)T	The following keywords and arguments were added: **consent**, **absolute-timer,** *minutes*, **inactivity-time**, *minutes,* **parameter-map**, and *consent-parameter-map-name*.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The admission rule defines how you apply admission control.

You can associate the named rule with an ACL, providing control over which hosts use the admission control feature. If no standard access list is defined, the named admission rule intercepts IP traffic from all hosts whose connection-initiating packets are received at the configured interface.

The **bypass** keyword allows an administrator the choice of not having to use the EAPoUDP-based posture validation for the hosts that are trying to connect on the port. The bypass can be used if an administrator knows that the hosts that are connected on the port do not have the Cisco Trust Agent client installed.

The **service-policy type tag** {*service-policy-name*} keywords and argument allow you to associate the service policy of the type tag with the IP admission rule. On the network access device (NAD), a set of policies can be associated with an arbitrary tag string, and if the AAA server sends the same tag in response to the posture validation or authentication response, the policies that are associated with the tag can be applied on the host. The **service policy** keyword is an optional keyword, and if the service policy is not associated with the IP admission name, the policies that are received from the AAA server are applied on the host.

The **list** keyword option allows you to apply a standard, extended (1 through 199) or named access list to a named admission control rule. IP connections that are initiated by hosts in the access list are intercepted by the admission control feature.

The **event** keyword option allows you to specify the condition that triggered application of an identity policy.

The **timeout aaa** keyword option specifies that the AAA server is unreachable, and this condition is triggering the application of an identity policy.

The **policy identity** keyword and the *identity-policy-name* argument allow you to configure application of an identity policy and specify the policy type to be applied while the AAA server is unreachable.

The **consent** keyword and the **parameter-map** *consent-parameter-map-name* keyword and argument allow you to associate the authentication proxy consent feature with an IP admission rule. The consent feature enables customers to display a consent webpage to an end user, providing access to wireless services only after the end user accepts the agreement.

Examples

"Tag and Template" Feature Examples

The following example shows that an IP admission control rule is named "greentree" and that it is associated with ACL "101." Any IP traffic that is destined to a previously configured network (using the **access-list** command) will be subjected to antivirus state validation using EAPoUDP.

```
Router (config)# ip admission name greentree eapoudp list 101
```

The following example shows that EAPoUDP bypass has been configured:

```
Router (config)# ip admission name greentree eapoudp bypass list 101
```

In the following service policy example, tags named "healthy" and "non_healthy" can be received from an AAA server, the policy map is defined on the NAD, and the tag policy type is associated with the IP admission name "greentree."

Class Map Definition for the "healthy class" Type Tag

```
Router (config)# class-map type tag healthy_class
Router(config-cmap)# match tag healthy
Router(config-cmap)# end
```

Class Map Definition for the "non_healthy_class" Type Tag

```
Router (config)# class-map type tag non_healthy_class
Router (config-cmap)# match tag non_healthy
Router (config-cmap)# end
```

Policy Map Definition

```
! The following line will be associated with the IP admission name.
Router (config)# policy-map type control tag global_class
! The following line refers to the healthy class map that was defined above.
Router (config-pmap)# class healthy_class
Router (config-pmap-c)# identity policy healthy_policy
Router(config-pmap-c)# exit
The following line refers to the non_healthy class that was defined above.
Router (config-pmap)# class non_healthy_class
Router(config-pmap-c)# identity policy non_healthy_policy
Router (config-pmap-c)# end
```

Identity Policy Definition

```
Router (config)# identity policy healthy_policy
```

```
! The following line is the IP access list for healthy users.
Router (config-identity-policy)# access-group healthy
Router (config-identity-policy)# end
Router (config)# identity policy non_healthy_policy
Router (config-identity-policy)# access-group non_healthy
Router (config-identity-policy)# end
```

Defining Access Lists

```
Router (config)# ip access-list extended healthy_class
! The following line can be anything, but as an example, traffic is being allowed.
Router (config-ext-nacl)# permit ip any any
Router (config-ext-nac)# end
Router (config)# ip access-list extended non_healthy_class
! The following line is only an example. In practical cases, you could prevent a user from
accessing specific networks.
Router (config-ext-nacl)# deny ip any any
Router (config-ext-nac)# end
```

Associating the Policy Map with the IP Admission Name

```
Router (config)# ip admission name greentree service-policy type tag global_class
! In the next line, the admission name can be associated with the interface.
Router (config)# interface fastethernet 1/0
Router (config-if)# ip admission greentree
```

In the above configuration, if the AAA server sends a tag named "healthy" or "non_healthy" for any host, the policies that are associated with the appropriate identity policy will be applied on the host.

NAC—Auth Fail Open Feature Examples

The following example shows how to define an IP admission control rule named “samplerule” and attach it to a specific interface:

```
Router (config)# ip admission name samplerule eapoudp list 101 event timeout aaa policy
identity aaa_fail_policy
Router (config)# interface fastethernet 1/1
Router (config-if)# ip admission samplerule
Router (config-if)# end
```

In the above configuration, if the specified interface is not already authorized when the AAA server becomes unreachable, it will operate under the specified policy until revalidation is possible.

Authentication Proxy Consent Webpage Example

The following example shows how to configure an IP admission consent rule and associate the consent rule with the definitions of the parameter map “consent_parameter_map”:

```
ip admission name consent-rule consent inactivity-time 204 absolute-timer 304
parameter-map consent_parameter_map list 103
ip admission consent-banner file flash:consent_page.html
ip admission consent-banner text ^C Consen-Page-Banner-Text ^C
ip admission max-login-attempts 5
ip admission init-state-timer 15
ip admission auth-proxy-audit
ip admission inactivity-timer 205
ip admission absolute-timer 305
ip admission ratelimit 100
ip http server
ip http secure-server
!
interface FastEthernet 0/0
 description ### CLIENT-N/W ###
 ip address 192.168.100.170 255.255.255.0
```

```
 ip access-group 102 in
 ip admission consent-rule
 no shut
 exit
!
interface FastEthernet 0/1
 description ### AAA-DHCP-AUDIT-SERVER-N/W ###
 ip address 192.168.104.170 255.255.255.0
 no shut
 exit
!
line con 0
 exec-timeout 0 0
 login authentication noAAA
 exit
!
line vty 0 15
 exec-timeout 0 0
 login authentication noAAA
 exit
!
```

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
ip admission event timeout aaa policy identity	Defines a policy to be applied when the AAA server is unreachable.

ip admission proxy http

To specify the display of custom authentication proxy web pages during web-based authentication, use the **ip admission proxy http** command in global configuration mode. To specify the use of the default web page, use the **no** form of this command.

ip admission proxy http {{**login** | **success** | **failure** | **login expired**} **page file** *device*:*file-name*} | {**success redirect** *url*}}

no ip admission proxy http {{**login** | **success** | **failure** | **login expired**} **page file** *device*:*file-name*} | {**success redirect** *url*}}

Syntax Description

login	Specifies a locally stored web page to be displayed during login.
success	Specifies a locally stored web page to be displayed when the login is successful.
failure	Specifies a locally stored web page to be displayed when the login has failed.
login expired	Specifies a locally stored web page to be displayed when the login has expired.
device	Specifies a disk or flash memory in the switch memory file system where the custom HTML file is stored.
file-name	Specifies the name of the custom HTML file to be used in place of the default HTML file for the specified condition.
success redirect *url*	Specifies an external web page to be displayed when the login is successful.

Command Default

The internal default authentication proxy web pages are displayed during web-based authentication.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

When configuring the use of customized authentication proxy web pages, consider the following guidelines:

- To enable the custom web pages feature, you must specify all four custom HTML files. If fewer than four files are specified, the internal default HTML pages will be used.
- The four custom HTML files must be present on the disk or flash of the switch. The maximum size of each HTML file is 8 KB.
- Any images on the custom pages must be located on an accessible HTTP server. An intercept ACL must be configured within the admission rule to allow access to the HTTP server.
- Any external link from a custom page will require configuration of an intercept ACL within the admission rule.

- Any name resolution required for external links or images will require configuration of an intercept ACL within the admission rule to access a valid DNS server.
- If the custom web pages feature is enabled, a configured auth-proxy-banner will not be used.
- If the custom web pages feature is enabled, the redirection URL for successful login feature will not be available.
- Because the custom login page is a public web form, consider the following guidelines for this page:
  - The login form must accept user input for the username and password and must POST the data as uname and pwd.
  - The custom login page should follow best practices for a web form, such as page timeout, hidden password, and prevention of redundant submissions.
- When configuring a redirection URL for successful login, consider the following guidelines:
  - If the custom authentication proxy web pages feature is enabled, the redirection URL feature is disabled and will not be available in the CLI. You can perform redirection in the custom login success page.
  - If the redirection URL feature is enabled, a configured auth-proxy-banner will not be used.

Examples

The following example shows how to configure custom authentication proxy web pages:

```
Router(config)# ip admission proxy http login page file disk1:login.htm
Router(config)# ip admission proxy http success page file disk1:success.htm
Router(config)# ip admission proxy http fail page file disk1:fail.htm
Router(config)# ip admission proxy http login expired page file disk1:expired.htm
```

The following example shows how to verify the configuration of custom authentication proxy web pages:

```
Router# show ip admission configuration

Authentication proxy webpage
 Login page         : disk1:login.htm
 Success page       : disk1:success.htm
 Fail Page          : disk1:fail.htm
 Login expired Page : disk1:expired.htm

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

The following example shows how to configure a redirection URL for successful login:

```
Router(config)# ip admission proxy http success redirect www.example.com
```

The following example shows how to verify the redirection URL for successful login:

```
Router# show ip admission configuration

Authentication Proxy Banner not configured
Customizable Authentication Proxy webpage not configured
HTTP Authentication success redirect to URL: http://www.example.com
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is disabled
```

```
Authentication Proxy Max HTTP process is 7
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

Related Commands

Command	Description
ip http server **ip https server**	Enables the HTTP server within the switch.
show ip admission configuration	Displays the configuration of web-based authentication ip admission.

ip audit

To apply an audit specification created with the **ip audit** command to a specific interface and for a specific direction, use the **ip audit** command in interface configuration mode. To disable auditing of the interface for the specified direction, use the **no** version of this command.

ip audit *audit-name* {**in** | **out**}

no ip audit *audit-name* {**in** | **out**}

Syntax Description

audit-name	Name of an audit specification.
in	Inbound traffic.
out	Outbound traffic.

Defaults

No audit specifications are applied to an interface or direction.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ip audit** interface configuration command to apply an audit specification created with the **ip audit** command to a specific interface and for a specific direction.

Examples

In the following example, the audit specification MARCUS is applied to an interface and direction:

```
interface e0
 ip audit MARCUS in
```

In the following example, the audit specification MARCUS is removed from the interface on which it was previously added:

```
interface e0
 no ip audit MARCUS in
```

ip audit attack

To specify the default actions for attack signatures, use the **ip audit attack** command in global configuration mode. To set the default action for attack signatures, use the **no** form of this command.

ip audit attack {**action** [**alarm**] [**drop**] [**reset**]}

no ip audit attack

Syntax Description

action	Specifies an action for the attack signature to take in response to a match.
alarm	(Optional) Sends an alarm to the console, NetRanger Director, or to a syslog server. Used with the **action** keyword.
drop	(Optional) Drops the packet. Used with the **action** keyword.
reset	(Optional) Resets the TCP session. Used with the **action** keyword.

Defaults

The default action is **alarm**.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ip audit attack** global configuration command to specify the default actions for attack signatures.

Examples

In the following example, the default action for attack signatures is set to all three actions:

```
ip audit attack action alarm drop reset
```

ip audit info

To specify the default actions for info signatures, use the **ip audit info** command in global configuration mode. To set the default action for info signatures, use the **no** form of this command.

ip audit info {**action** [**alarm**] [**drop**] [**reset**]}

no ip audit info

Syntax Description

action	Sets an action for the info signature to take in response to a match.
alarm	(Optional) Sends an alarm to the console, NetRanger Director, or to a syslog server. Used with the **action** keyword.
drop	(Optional) Drops the packet. Used with the **action** keyword.
reset	(Optional) Resets the TCP session. Used with the **action** keyword.

Defaults

The default action is **alarm**.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ip audit info** global configuration command to specify the default actions for info signatures.

Examples

In the following example, the default action for info signatures is set to all three actions:

```
ip audit info action alarm drop reset
```

ip audit name

To create audit rules for info and attack signature types, use the **ip audit name** command in global configuration mode. To delete an audit rule, use the **no** form of this command.

ip audit name *audit-name* {**info** | **attack**} [**list** *standard-acl*] [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit name *audit-name* {**info** | **attack**}

Syntax Description

audit-name	Name for an audit specification.
info	Specifies that the audit rule is for info signatures.
attack	Specifies that the audit rule is for attack signatures.
list	(Optional) Specifies an ACL to attach to the audit rule.
standard-acl	(Optional) Integer representing an access control list. Use with the **list** keyword.
action	(Optional) Specifies an action or actions to take in response to a match.
alarm	(Optional) Sends an alarm to the console, NetRanger Director, or to a syslog server. Use with the **action** keyword.
drop	(Optional) Drops the packet. Use with the **action** keyword.
reset	(Optional) Resets the TCP session. Use with the **action** keyword.

Defaults

If an action is not specified, the default action is **alarm**.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Any signatures disabled with the **ip audit signature** command do not become a part of the audit rule created with the **ip audit name** command.

Examples

In the following example, an audit rule called INFO.2 is created, and configured with all three actions:

```
ip audit name INFO.2 info action alarm drop reset
```

In the following example, an info signature is disabled and an audit rule called INFO.3 is created:

```
ip audit signature 1000 disable
```

```
ip audit name INFO.3 info action alarm drop reset
```

In the following example, an audit rule called ATTACK.2 is created with an attached ACL 91, and the ACL is created:

```
ip audit name ATTACK.2 list 91
access-list 91 deny 10.1.0.0 0.0.255.255
access-list 91 permit any
```

ip audit notify

To specify the method of event notification, use the **ip audit notify** command in global configuration mode. To disable event notifications, use the **no** form of this command.

ip audit notify {**nr-director** | **log**}

no ip audit notify {**nr-director** | **log**}

Syntax Description

nr-director	Send messages in NetRanger format to the NetRanger Director or Sensor.
log	Send messages in syslog format.

Defaults

The default is to send messages in syslog format.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If messages are sent to the NetRanger Director, then you must also configure the NetRanger Director's Post Office transport parameters using the **ip audit po remote** command.

Examples

In the following example, event notifications are specified to be sent in NetRanger format:

```
ip audit notify nr-director
```

Related Commands

Command	Description
ip audit po local	Specifies the local Post Office parameters used when sending event notifications to the NetRanger Director.
ip audit po remote	Specifies one or more sets of Post Office parameters for NetRanger Directors receiving event notifications from the router.

ip audit po local

To specify the local Post Office parameters used when sending event notifications to the NetRanger Director, use the **ip audit po local** command in global configuration mode. To set the local Post Office parameters to their default settings, use the **no** form of this command.

ip audit po local hostid *id-number* **orgid** *id-number*

no ip audit po local [**hostid** *id-number* **orgid** *id-number*]

Syntax Description

hostid	Specifies a NetRanger host ID.
id-number	Unique integer in the range 1 to 65535 used in NetRanger communications to identify the local host. The default host ID is 1.
orgid	Specifies a NetRanger organization ID.
id-number	Unique integer in the range 1 to 65535 used in NetRanger communications to identify the group to which the local host belongs. The default organization ID is 1.

Defaults

The default organization ID is 1. The default host ID is 1.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ip audit po local** global configuration command to specify the local Post Office parameters used when sending event notifications to the NetRanger Director.

Examples

In the following example, the local host is assigned a host ID of 10 and an organization ID of 500:

```
ip audit po local hostid 10 orgid 500
```

ip audit po max-events

To specify the maximum number of event notifications that are placed in the router's event queue, use the **ip audit po max-events** command in global configuration mode. To set the number of recipients to the default setting, use the **no** version of this command.

ip audit po max-events *number-of-events*

no ip audit po max-events

Syntax Description

number-of-events	Integer in the range from 1 to 65535 that designates the maximum number of events allowable in the event queue. The default is 100 events.

Defaults

The default number of events is 100.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Raising the number of events past 100 may cause memory and performance impacts because each event in the event queue requires 32 KB of memory.

Examples

In the following example, the number of events in the event queue is set to 250:

```
ip audit po max-events 250
```

ip audit po protected

To specify whether an address is on a protected network, use the **ip audit po protected** command in global configuration mode. To remove network addresses from the protected network list, use the **no** form of this command.

ip audit po protected *ip-addr* [**to** *ip-addr*]

no ip audit po protected [*ip-addr*]

Syntax Description

ip-addr	IP address of a network host.
to *ip-addr*	(Optional) Specifies a range of IP addresses.

Defaults

If no addresses are defined as protected, then all addresses are considered outside the protected network.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can enter a single address at a time or a range of addresses at a time. You can also make as many entries to the protected networks list as you want. When an attack is detected, the corresponding event contains a flag that denotes whether the source or destination of the packet belongs to a protected network or not.

If you specify an IP address for removal, that address is removed from the list. If you do not specify an address, then all IP addresses are removed from the list.

Examples

In the following example, a range of addresses is added to the protected network list:

```
ip audit po protected 10.1.1.0 to 10.1.1.255
```

In the following example, three individual addresses are added to the protected network list:

```
ip audit po protected 10.4.1.1
ip audit po protected 10.4.1.8
ip audit po protected 10.4.1.25
```

In the following example, an address is removed from the protected network list:

```
no ip audit po protected 10.4.1.1
```

ip audit po remote

To specify one or more set of Post Office parameters for NetRanger Directors receiving event notifications from the router, use the **ip audit po remote** global configuration command. To remove a NetRanger Director's Post Office parameters as defined by host ID, organization ID, and IP address, use the **no** form of this command.

ip audit po remote hostid *host-id* **orgid** *org-id* **rmtaddress** *ip-address* **localaddress** *ip-address* [**port** *port-number*] [**preference** *preference-number*] [**timeout** *seconds*] [**application** {**director** | **logger**}]

no ip audit po remote hostid *host-id* **orgid** *org-id* **rmtaddress** *ip-address*

Syntax Description

host-id	Unique integer in the range from 1 to 65535 used in NetRanger communications to identify the local host. Use with the **hostid** keyword.
hostid	Specifies a NetRanger host ID.
org-id	Unique integer in the range from 1 to 65535 used in NetRanger communications to identify the group in which the local host belongs. Use with the **orgid** keyword.
orgid	Specifies a NetRanger organization ID.
rmtaddress	Specifies the IP address of the NetRanger Director.
localaddress	Specifies the IP address of the Cisco IOS Firewall IDS router.
ip-address	IP address of the NetRanger Director or Cisco IOS Firewall IDS router's interface. Use with the **rmtaddress** and **localaddress** keywords.
port-number	(Optional) Integer representing the UDP port on which the NetRanger Director is listening for event notifications. Use with the **port** keyword.
port	(Optional) Specifies a User Datagram Protocol port through which to send messages.
preference	(Optional) Specifies a route preference for communication.
preference-number	(Optional) Integer representing the relative priority of a route to a NetRanger Director, if more than one route exists. Use with the **preference** keyword.
seconds	(Optional) Integer representing the heartbeat timeout value for Post Office communications. Use with the **timeout** keyword.
timeout	(Optional) Specifies a timeout value for Post Office communications.
application	(Optional) Specifies the type of application that is receiving the Cisco IOS Firewall IDS messages.
director	(Optional) Specifies that the receiving application is the NetRanger Director interface.
logger	(Optional) Specifies that the receiving application is a NetRanger Sensor.

Defaults

The default organization ID is 1.

The default host ID is 1.

The default UDP port number is 45000.

The default preference is 1.

The default heartbeat timeout is 5 seconds.

The default application is **director**.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A router can report to more than one NetRanger Director. In this case, use the **ip audit po remote** command to add each NetRanger Director to which the router sends notifications.

More than one route can be established to the same NetRanger Director. In this case, you must give each route a preference number that establishes the relative priority of routes. The router always attempts to use the lowest numbered route, switching automatically to the next higher number when a route fails, and then switching back when the route begins functioning again.

A router can also report to a NetRanger Sensor. In this case, use the **ip audit po remote** command and specify **logger** as the application.

Examples

In the following example, two communication routes for the same dual-homed NetRanger Director are defined:

```
ip audit po remote hostid 30 orgid 500 rmtaddress 10.1.99.100 localaddress 10.1.99.1
preference 1
ip audit po remote hostid 30 orgid 500 rmtaddress 10.1.4.30 localaddress 10.1.4.1
preference 2
```

The router uses the first entry to establish communication with the NetRanger Director defined with host ID 30 and organization ID 500. If this route fails, then the router will switch to the secondary communications route. As soon as the first route begins functioning again, the router switches back to the primary route and closes the secondary route.

In the following example, a different Director is assigned a longer heartbeat timeout value because of network congestion, and is designated as a logger application:

```
ip audit po remote hostid 70 orgid 500 rmtaddress 10.1.8.1 localaddress 10.1.8.100 timeout
10 application director
```

ip audit signature

To attach a policy to a signature, use the **ip audit signature** command in global configuration mode. To remove the policy, use the **no** form of this command. If the policy disabled a signature, then the **no** form of this command reenables the signature. If the policy attached an access list to the signature, the **no** form of this command removes the access list.

ip audit signature *signature-id* {**disable** | **list** *acl-list*}

no ip audit signature *signature-id*

Syntax Description

signature-id	Unique integer specifying a signature as defined in the NetRanger Network Security Database.
disable	Disables the ACL associated with the signature.
list	Specifies an ACL to associate with the signature.
acl-list	Unique integer specifying a configured ACL on the router. Use with the **list** keyword.

Defaults

No policy is attached to a signature.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command allow you to set two policies: disable the audit of a signature or qualify the audit of a signature with an access list.

If you are attaching an access control list to a signature, then you also need to create an audit rule with the **ip audit name** command and apply it to an interface with the **ip audit** command.

Examples

In the following example, a signature is disabled, another signature has ACL 99 attached to it, and ACL 99 is defined:

```
ip audit signature 6150 disable
ip audit signature 1000 list 99

access-list 99 deny 10.1.10.0 0.0.0.255
access-list 99 permit any
```

ip audit smtp

To specify the number of recipients in a mail message over which a spam attack is suspected, use the **ip audit smtp** command in global configuration mode. To set the number of recipients to the default setting, use the **no** form of this command.

ip audit smtp spam *number-of-recipients*

no ip audit smtp spam

Syntax Description

spam	Specifies a threshold beyond which the Cisco IOS Firewall IDS alarms on spam e-mail.
number-of-recipients	Integer in the range of 1 to 65535 that designates the maximum number of recipients in a mail message before a spam attack is suspected. Use with the **spam** keyword. The default is 250 recipients.

Defaults

The default number of recipients is 250.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ip audit smtp** global configuration command to specify the number of recipients in a mail message over which a spam attack is suspected.

Examples

In the following example, the number of recipients is set to 300:

```
ip audit smtp spam 300
```

ip auth-proxy (global configuration)

To set the the authentication proxy idle timeout or maximum number of idle connections, use the **ip auth-proxy** command in global configuration mode. To return the idle timeout or maximum number of idle connections to their default values, use the **no** form of this command.

ip auth-proxy {**absolute-timer** *min* | **inactivity-timer** *min* | **init-state-timer** *min*| **max-nodata-conns** *number*}

no ip auth-proxy [**absolute-timer**] [**inactivity-timer**] [**init-state-timer**] [**max-nodata-conns**]

Syntax Description

absolute-timer *min*	Length of time in minutes that an ingress IP authentication proxy session can remain active. After this timer expires, each session must go through the entire process of establishing its connection as if it was a new request. The range is 0 to 35,791. The default is 0.
inactivity-timer *min*	Length of time in minutes that an active ingress session can be present with no activity or data from the end client. If this timer expires without activity or data, the session is cleared. The range is 1 to 2,147,483,647. The default is 60. **Note** This keyword and argument pair replaces the **auth-cache-time** *min* keyword and argument pair.
init-state-timer *min*	Length of time in minutes that an ingress authentication proxy session can stay in the INIT state. An ingress session is first registered in the INIT state until the user enters their username and password credentials. If the timer expires before the credentials are entered, the session is removed. The range is 1 to 15. The default is 2.
max-nodata-conns *number*	Maximum number of idle (“no data”) TCP connections that can exist globally for the IP authentication feature. The range is 1 to 1,000. The default is 3.

Command Default

The absolute timer is enabled indefinitely. The inactivity timer, and the INIT state timer are enabled. The limit on the number of global idle TCP connections is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(1)	The **inactivity-timer** and **absolute-timer** keywords were added.
12.4(6)T	The **init-state-timer** keyword was added
12.2(33)SRA	This command was integrated into Cisco IOS release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You use the **ip auth-proxy** command to set the global idle timeout value for the authentication proxy. The idle timeout value is the length of time an authentication cache entry, along with its associated dynamic user access control list, is cleared after a period of inactivity.

You use the **absolute-timer** keyword to configure the length of time during which the authentication proxy on the enabled interface is active. After the absolute timer expires, the authentication proxy is disabled regardless of any activity. You can override the global absolute timeout value with the local (per protocol) value, which you can enable by using the **ip auth-proxy name** command. The absolute timer is turned off by default, and the authentication proxy is enabled indefinitely.

You must set the value of the **inactivity-timer** keyword to a higher value than the idle timeout of any Context-Based Access Control (CBAC) protocols. Otherwise, when the authentication proxy removes the user profile (and its associated dynamic user ACLs), there might be idle connections monitored by CBAC. Removing these user-specific ACLs could cause those idle connections to hang. If the CBAC idle timeout value is shorter, CBAC resets these connections when the CBAC idle timeout expires, which is before the authentication proxy removes the user profile.

You use the **init-state-timer** keyword to configure the amount of time that the authentication proxy is allowed to clear connections that are in the INIT state. Authentication attempts can remain in the INIT state when the router is loaded heavily and the authentication is not completed in two minutes. This problem is more likely if HTTPS is used for authenticating users. The default value of two minutes is usually sufficient to handle most cases, but if not, you should use the **init-state-timer** keyword to increase this value.

You use the **max-nodata-conns** keyword to limit the number of idle TCP connections (TCP sessions that are active but do not transmit data for a long period of time). There is no timer associated with this number.

Examples

The following example sets the inactivity timer to 30 minutes:

```
Router> enable
Router# configure terminal
Router(config)# ip auth-proxy inactivity-timer 30
```

The following example sets the INIT state timer to 15 minutes:

```
Router> enable
Router# configure terminal
Router(config)# ip auth-proxy init-state-timer 15
```

Related Commands

Command	Description
ip auth-proxy name	Creates an authentication proxy rule.
show ip auth-proxy configuration	Displays the authentication proxy entries or the running authentication proxy configuration.

ip auth-proxy (interface configuration)

To apply an authentication proxy rule at a firewall interface, use the **ip auth-proxy** command in interface configuration mode. To remove the authentication proxy rules, use the **no** form of this command.

ip auth-proxy *auth-proxy-name*

no ip auth-proxy *auth-proxy-name*

Syntax Description

auth-proxy-name	Specifies the name of the authentication proxy rule to apply to the interface configuration. The authentication proxy rule is established with the **ip auth-proxy name** command.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ip auth-proxy** command to enable the named authentication proxy rule at the firewall interface. Traffic passing through the interface from hosts with an IP address matching the standard access list and protocol type (HTTP) is intercepted for authentication if no corresponding authentication cache entry exists. If no access list is defined, the authentication proxy intercepts traffic from all hosts whose connection initiating packets are received at the configured interface.

Use the **no** form of this command with a rule name to disable the authentication proxy for a given rule on a specific interface. If a rule is not specified, the **no** form of this command disables the authentication proxy on the interface.

Examples

The following example configures interface Ethernet0 with the HQ_users rule:

```
interface e0
 ip address 172.21.127.210 255.255.255.0
 ip access-group 111 in
 ip auth-proxy HQ_users
 ip nat inside
```

Related Commands

Command	Description
ip auth-proxy name	Creates an authentication proxy rule.

ip auth-proxy auth-proxy-banner

To display a banner, such as the router name, in the authentication proxy login page, use the **ip auth-proxy auth-proxy-banner** command in global configuration mode. To disable display of the banner, use the **no** form of this command.

ip auth-proxy auth-proxy-banner {**ftp** | **http** | **telnet**} [*banner-text*]

no ip auth-proxy auth-proxy-banner {**ftp** | **http** | **telnet**}

Syntax Description

ftp	Specifies the FTP protocol.
http	Specifies the HTTP protocol.
telnet	Specifies the Telnet protocol.
banner-text	(Optional) Specifies a text string to replace the default banner, which is the name of the router. The text string should be written in the following format: "C banner-text C," where "C" is a delimiting character.

Defaults

This command is not enabled, and a banner is not displayed on the authentication proxy login page.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(1)	The following keywords were added: **ftp**, **http**, and **telnet**.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **ip auth-proxy auth-proxy-banner** command allows users to configure one of two possible scenarios:

- The **ip auth-proxy auth-proxy-banner** command is enabled.

  In this scenario, the administrator has not supplied any text. Thus, a default banner that states the following: "Cisco Systems, <router's hostname> Authentication" will be displayed in the authentication proxy login page. This scenario is most commonly used.

- The **ip auth-proxy auth-proxy-banner** command with the *banner-text* argument is enabled.

  In this scenario, the administrator can supply multiline text that will be converted to HTML by the auth-proxy parser code. Thus, *only* the multiline text will displayed in the authentication proxy login page. You will *not* see the default banner, "Cisco Systems, <router's hostname> Authentication."

Note If the **ip auth-proxy auth-proxy-banner** command is not enabled, there will not be any banner configuration. Thus, nothing will be displayed to the user on authentication proxy login page except a text box to enter the username and a text box to enter the password.

Examples

The following example causes the router name to be displayed in the authentication proxy login page:

```
ip auth-proxy auth-proxy-banner ftp
```

The following example shows how to specify the custom banner “whozat” to be displayed in the authentication proxy login page:

```
ip auth-proxy auth-proxy-banner telnet CwhozatC
```

Related Commands

Command	Description
ip auth-proxy name	Creates an authentication proxy rule.

ip auth-proxy max-login-attempts

To limit the number of login attempts at a firewall interface in the interface configuration command mode, use the **ip auth-proxy max-login-attempts** command. Use the **no** form of this command to return to the default settings.

ip auth-proxy max-login-attempts *number*

no ip auth-proxy max-login-attempts

Syntax Description

number	Maximum number of login attempts. The range is 1 to 2147483647. The default value depends on the authentication mechanism: • FTP: 5 • HTTP: 30 • Telnet: 3

Defaults

Enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 only.

This command is supported on the firewall interfaces only.

The maximum login attempt functionality is independent of the watch-list feature. (You create a watch list with the **ip access-list hardware permit fragments** command.) If you do not configure a watch list, the existing authentication proxy behavior occurs, but it displays the new number for retries. If you configure a watch list, when the maximum is reached, the session is blocked and the IP address is put in the watch list.

Examples

This example shows how to set a limit to the number of login attempts at a firewall interface:

```
Router(config-if)# ip auth-proxy max-login-attempts 4
Router(config-if)#
```

Related Commands

Command	Description
clear ip auth-proxy watch-list	Deletes a single watch-list entry or all watch-list entries.
ip auth-proxy watch-list	Enables and configures an authentication proxy watch list.
show ip auth-proxy watch-list	Displays the information about the authentication proxy watch list.

ip auth-proxy name

To create an authentication proxy rule, use the **ip auth-proxy name** command in global configuration mode. To remove the authentication proxy rules, use the **no** form of this command.

Cisco IOS 12.4(6)T and Later Releases

ip auth-proxy name *auth-proxy-name* {**ftp** | **http** | **telnet**} [**event timeout aaa policy identity** *id-policy-name*] [**absolute-timer** *timeout*] [**auth-cache-time** *timeout*] [**inactivity-time** *timeout*] [**list** {*list-num* [**service-policy type tag** *policy-name*] | *std-list-num* | *list-name*}] [**service-policy type tag** *service-policy-name*]

no ip auth-proxy name *auth-proxy-name* {**ftp** | **http** | **telnet**}

Cisco IOS Release 12.2(33)SRA, 12.2SX, and Later Releases

ip auth-proxy name *auth-proxy-name* {**ftp** | **http** | **telnet**} [**event timeout aaa policy identity** *id-policy-name*] [**absolute-timer** *timeout*] [**auth-cache-time** *timeout*] [**inactivity-time** *timeout*] [**list** {*list-num* | *std-list-num* | *list-name*}]

no ip auth-proxy name *auth-proxy-name* {**ftp** | **http** | **telnet**}

Syntax Description

auth-proxy-name	A name of up to 16 alphanumeric characters to be associated with an authentication proxy rule.
ftp	Specifies FTP to trigger the authentication proxy.
http	Specifies HTTP to trigger the authentication proxy.
telnet	Specifies Telnet to trigger the authentication proxy.
event timeout aaa policy identity *id-policy-name*	(Optional) Specifies the event to be associated with the policy, timeout of the based event, AAA fail policy to be applied, Identity fail policy to be applied, and Identity policy name.
absolute-timer *timeout*	(Optional) Specifies a window in which the authentication proxy on the enabled interface is active. Enter a value in the range 0 to 35791 minutes. The default value is 0 minutes.
auth-cache-time *timeout*	(Optional) Alias of inactivity timeout in minutes. Enter a value in the range 1 to 35791 minutes.
inactivity-time *min*	(Optional) Overrides the global authentication proxy cache timer for a specific authentication proxy name, offering more control over timeout values. Enter a value in the range 1 to 35791 minutes. The default value is equal to the value set with the **ip auth-proxy** command. **Note** This option deprecates the **auth-cache-time** *timeout* option.
list {*list-num* | *std-list-num* | *list-name*}	(Optional) Specifies a standard (1 to 99), extended (1 to 199), or named IP access list to use with the authentication proxy. With this option, the authentication proxy is applied only to those hosts in the access list. If no list is specified, all connections initiating HTTP, FTP, or Telnet traffic arriving at the interface are subject to authentication.

service-policy type tag	(Optional) A control plane service policy is to be configured.
service-policy-name	(Optional) Control plane tag service policy that is configured using the **policy-map type control tag** *policy-map-name* command. This policy map is used to apply the actions on the host when a tag is received.

Command Default

The default value is equal to the value set with the **ip auth-proxy auth-cache-time** command.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2	Support for named and extend access lists was introduced.
12.3(1)	The following keywords were introduced: • **ftp** • **telnet** • **inactivity-time** *timeout* • **absolute-timer** *timeout*
12.4(6)T	The **service-policy type tag** keywords and *service-policy-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **event**, **timeout**, **aaa**, **policy**, **identity** keywords and the *id-policy-name* argument were added.

Usage Guidelines

This command creates a named authentication proxy rule, and it allows you to associate that rule with an access control list (ACL), providing control over which hosts use the authentication proxy. The rule is applied to an interface on a router using the **ip auth-proxy** command.

Use the **inactivity-time** *timeout* option to override the global the authentication proxy cache timer. This option provides control over timeout values for specific authentication proxy rules. The authentication proxy cache timer monitors the length of time (in minutes) that an authentication cache entry, along with its associated dynamic user access control list, is managed after a period of inactivity. When that period of inactivity (idle time) expires, the authentication entry and the associated dynamic access lists are deleted.

Use the **list** option to associate a set of specific IP addresses or a named ACL with the **ip auth-proxy name** command.

Use the **no** form of this command with a rule name to remove the authentication proxy rules. If no rule is specified, the **no** form of this command removes all the authentication rules on the router, and disables the proxy at all interfaces.

Note You must use the **aaa authorization auth-proxy** command with the **ip auth-proxy name** command. Together these commands set up the authorization policy to be retrieved by the firewall. Refer to the **aaa authorization auth-proxy** command for more information.

Examples

The following example shows how to create the HQ_users authentication proxy rule. Because an access list is not specified in the rule, all connection-initiating HTTP traffic is subjected to authentication.

```
ip auth-proxy name HQ_users http
```

The following example shows how to create the Mfg_users authentication proxy rule and apply it to hosts specified in ACL 10:

```
access-list 10 192.168.7.0 0.0.0.255
ip auth-proxy name Mfg_users http list 10
```

The following example shows how to set the timeout value for Mfg_users to 30 minutes:

```
access-list 15 any
ip auth-proxy name Mfg_users http inactivity-timer 30 list 15
```

The following example shows how to disable the Mfg_users rule:

```
no ip auth-proxy name Mfg_users
```

The following example shows how to disable the authentication proxy at all interfaces and remove all the rules from the router configuration:

```
no ip auth-proxy xyz ftp
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict network access to a user.
ip auth-proxy (global)	Sets the authentication proxy idle timeout value (that is, the length of time an authentication cache entry, along with its associated dynamic user ACL, is managed after a period of inactivity).
ip auth-proxy (interface)	Applies an authentication proxy rule at a firewall interface.
show ip auth-proxy configuration	Displays the authentication proxy entries or the running authentication proxy configuration.

ip auth-proxy watch-list

To enable and configure an authentication proxy watch list in the interface configuration command mode, use the **ip auth-proxy watch-list** command. To disable the watch-list functionality, remove an IP address from the watch list. Or, to return to the default setting, use the **no** form of this command.

ip auth-proxy watch-list {**add-item** *ip-addr* | **enable** | **expiry-time** *minutes*}

no ip auth-proxy watch-list [**add-item** *ip-addr* | **expiry-time**]

Syntax Description

add-item *ip-addr*	Adds an IP address to the watch list.
enable	Enables a watch list.
expiry-time *minutes*	Specifies the duration of time that an entry is in the watch list; see the "Usage Guidelines" section for valid values.

Defaults

The defaults are as follows:

- *minutes* is **30** minutes.
- The watch-list functionality is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 only.

The valid values for minutes are from 0 to the largest 32-bit positive number (0x7FFFFFFF or 2147483647 in decimal). Setting the *minutes* to 0 (zero) places the entries in the list permanently.

This command is supported on the firewall interfaces only.

Use the **no** form of this command to do the following:

- **no ip auth-proxy watch-list**—Disables the watch-list functionality.
- **no ip auth-proxy watch-list add-item** *ip-addr*—Removes the IP address from the watch list.
- **no ip auth-proxy watch-list expiry-time**—Returns to the default setting.

A watch list consists of IP addresses that have opened TCP connections to port 80 and have not sent any data. No new connections are accepted from this type of IP address (to port 80) and the packet is dropped.

An entry remains in the watch list for the time that is specified by **expiry-time** *minutes*.

When you disable a watch list, no new entries are put into the watch list, but the sessions are put in SERVICE_DENIED state. The timer deletes sessions after 2 minutes.

Examples

This example shows how to enable an authentication proxy watch list:

```
Router(config-if)# ip auth-proxy watch-list enable
Router(config-if)#
```

This example shows how to disable an authentication proxy watch list:

```
Router(config-if)# no ip auth-proxy watch-list
Router(config-if)#
```

This example shows how to add an IP address to a watch list:

```
Router(config-if)# ip auth-proxy watch-list add-item 10.0.0.2
Router(config-if)#
```

This example shows how to set the duration of time that an entry is in a watch list:

```
Router(config-if)# ip auth-proxy watch-list expiry-time 29
Router(config-if)#
```

Related Commands

Command	Description
clear ip auth-proxy watch-list	Deletes a single watch-list entry or all watch-list entries.
ip auth-proxy max-login-attempts	Limits the number of login attempts at a firewall interface.
show ip auth-proxy watch-list	Displays the information about the authentication proxy watch list.

ip dhcp client broadcast-flag (interface)

To configure a DHCP client to set or clear the broadcast flag, use the **ip dhcp client broadcast-flag** command in interface configuration mode. To disable the configuration, use the **no** form of this command.

ip dhcp client broadcast-flag {**clear** | **set**}

no ip dhcp client broadcast-flag

Syntax Description

clear	Clears the broadcast flag.
set	Sets the broadcast flag.

Command Default

The broadcast flag is set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

For a DHCP server to work on a Dynamic Multipoint VPN (DMVPN) network, the DHCP client available on the spoke must unicast the DHCP messages from the server to the client. By default, the DHCP client on the spoke broadcasts the DHCP messages. The broadcast flag is set during broadcast. Hence, the DHCP client on the spoke must have an option to clear the DHCP broadcast flag. You can use the **ip dhcp client broadcast-flag** command to configure the DHCP client to set or clear the broadcast flag.

Examples

The following example shows how to configure a DHCP client to clear the broadcast flag:

```
Router(config)# tunnel 1
Router(config-if)# ip dhcp client broadcast-flag clear
```

Related Commands

Command	Description
ip address dhcp	Acquires an IP address on an interface from the DHCP.
ip dhcp support tunnel unicast	Configures a spoke-to-hub tunnel to unicast the DHCP replies over the DMVPN network.

ip dhcp support tunnel unicast

To configure a spoke-to-hub tunnel to unicast DHCP replies over a Dynamic Multipoint VPN (DMVPN) network, use the **ip dhcp support tunnel unicast** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ip dhcp support tunnel unicast

no ip dhcp support tunnel unicast

Syntax Description

This command has no arguments or keywords.

Command Default

A spoke-to-hub tunnel broadcasts the replies over the DMVPN network.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

By default, the DHCP replies are broadcast from the DMVPN hub to the spoke. The DHCP relay agent must unicast the DHCP messages for a DHCP server to be functional in the DMVPN environment. Hence for the DHCP to be functional in DMVPN environment, you must configure the DHCP relay agent to unicast the DHCP messages.

Use the **ip dhcp support tunnel unicast** command to configure the DHCP relay agent to unicast the DHCP protocol messages from the server (hub) to the client (spoke). The relay agent uses the nonbroadcast multiaccess (NBMA) address to create temporary routes in Next Hop Resolution Protocol (NHRP) to help unicast the DHCPOFFER and DHCPACK messages to the spoke.

Examples

The following example shows how to configure a spoke-to-hub tunnel to unicast the replies over a DMVPN network:

```
Router(config)# ip dhcp support tunnel unicast
```

Related Commands

Command	Description
ip address dhcp	Configures an IP address on an interface acquired through DHCP.
ip dhcp client broadcast-flag	Configures the DHCP client to set or clear the broadcast flag.

ip-extension

To specify that IP extensions are included in a certificate request either for enrollment or generation of a certificate authority (CA) certificate for the Cisco IOS CA, use the **ip-extension** command in ca-trustpoint configuration mode. To remove a previously specified IP extension, use the **no** form of this command.

ip-extension [**multicast** | **unicast**] {**inherit** [**ipv4** | **ipv6**] | **prefix** *ipaddress* | **range** *min-ipaddress max-ipaddress*}

no ip-extension [**multicast** | **unicast**] {**inherit** [**ipv4** | **ipv6**] | **prefix** *ipaddress* | **range** *min-ipaddress max-ipaddress*}

Syntax Description

multicast	(Optional) Specifies that only multicast traffic, a subsequent address family identifier (SAFI), will be included in certificate requests.  **Note** If neither multicast nor unicast traffic is specified, both will be included in a certificate request.
unicast	(Optional) Specifies that only unicast traffic, a SAFI, will be included in certificate requests.  **Note** If neither multicast nor unicast traffic is specified, both will be included in a certificate request.
inherit	Specifies that IP addresses will be inherited from an issuer certificate. The issuer's certificate is first checked to find a certificate containing the address range or prefix. If no match is found, the certificate from the next issuer in the chain is checked, and so forth, up the certificate chain, recursively, until a match is located.
ipv4	(Optional) Specifies that only IPv4 addresses are inherited.  **Note** If neither an **ipv4** nor an **ipv6** address is specified, both address families are inherited.
ipv6	(Optional) Specifies that only IPv6 addresses are inherited.  **Note** If neither an **ipv4** nor an **ipv6** address is specified, both address families are inherited.

prefix *ipaddress*	Specifies the IP address prefix or a single IP address for either an IPv4 or IPv6 address. The IP address formats are: • A.B.C.D IPv4 address • A.B.C.D/nn IPv4 prefix • X:X:X:X::X IPv6 address • X:X:X:X::X/<0-128> IPv6 prefix
range	Specifies that there is a range of IP addresses.
min-ipaddress	The beginning IP address in the IP address range, in either IPv4 or IPv6 address format. The IP address formats are: • A.B.C.D Beginning IPv4 address in the range • X:X:X:X::X Beginning IPv6 address in the range
max-ipaddress	The ending IP address in the IP address range, in either IPv4 or IPv6 address format. The IP address formats are: • A.B.C.D Ending IPv4 address in the range • X:X:X:X::X Ending IPv6 address in the range

Command Default

No IP extensions will be included in a certificate request.

Command Modes

Ca-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
12.4(22)T	This command was introduced.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

The **ip-extension** command may be used to specify IP extensions for a public key infrastructure (PKI) server or client and may be issued one or more times, including multiple issuances with the **inherit**, **prefix**, and **range** keywords. For the inherit option, if the address family is not specified, both IPv4 and IPv6 addresses will be inherited. When the IPv4 or IPv6 address family is not specified for prefix or range, the address family will be determined from the address format.

Note It is recommended that you validate each **ip-extension** command line against your existing IP-extension configuration according to RFC 3779, verifying that IP address ranges do not overlap. The issue's certificate may not be available to validate the issuer's certificate for subsets of addresses.

Examples

The following example shows how to specify that multiple IP extensions are included in the server certificate request:

```
Router(ca-trustpoint)# ip-extension multicast prefix 10.64.0.0/11

! Only multicast traffic with the IPv4 prefix 10.64.0.0/11 will be included in certificate
requests.

Router(ca-trustpoint)# ip-extension prefix 2001:100:1::/48

! Multicast and unicast traffic with the IPv6 prefix 2001:100:1::/48 will be included in
certificate requests.

Router(ca-trustpoint)# ip-extension inherit

! Multicast and unicast traffic with IPv4 and IPv6 addresses will be inherited from the
issuer's certificate.

Router(ca-trustpoint)# ip-extension inherit ipv6

! Multicast and unicast traffic with IPv6 addresses only will be inherited from the
issuer's certificate.

Router(ca-trustpoint)# ip-extension unicast range 209.165.200.225 143.255.55.255

! Unicast traffic within the specified IPv4 address range will be included in the
certificate request.

Router(ca-trustpoint)# ip-extension range 2001:1:1::1 2001:1:2:ffff:ffff:ffff:ffff:ffff

! Multicast and unicast traffic within the specified IPv6 address range will be included
in the certificate request.
```

The following is sample output from the **show crypto pki certificates verbose** command. The output displays X.509 certificate IP address extension information where the IPv4 multicast prefix has been set to 10.64.0.0/11, and the IPv4 unicast range has been set to 209.165.201.1 209.165.201.30.

```
CA Certificate
   Status: Available
   Version: 3
   Certificate Serial Number (hex): 01
   Certificate Usage: Signature
   Issuer:
     cn=srtr1
   Subject:
     cn=srtr1
   Validity Date:
     start date: 21:50:11 PST Sep 29 2008
     end   date: 21:50:11 PST Sep 29 2011
   Subject Key Info:
     Public Key Algorithm: rsaEncryption
     RSA Public Key: (1024 bit)
   Signature Algorithm: MD5 with RSA Encryption
   Fingerprint MD5: 30C1C9B6 BC17815F DF6095CD EDE2A5F3
   Fingerprint SHA1: A67C451E 49E94E87 8EB0F71D 5BE642CF C68901EF
   X509v3 extensions:
     X509v3 Key Usage: 86000000
       Digital Signature
       Key Cert Sign
       CRL Signature
     X509v3 Subject Key ID: B593E52F F711094F 1CCAA4AE 683049AE 4ACE8E8C
```

```
  X509v3 Basic Constraints:
      CA: TRUE
  X509v3 Authority Key ID: B593E52F F711094F 1CCAA4AE 683049AE 4ACE8E8C
  Authority Info Access:
  X509v3 IP Extension:
      IPv4 (Unicast):
        209.165.202.129-209.165.202.158
      IPv4 (Multicast):
        10.64.0.0/11
Associated Trustpoints: srtr1
```

Related Commands

Command	Description
show crypto pki certificates	Displays information about the CA certificate.
show crypto pki trustpoints	Displays information about trustpoints that are configured on the router.

ip http ezvpn

To enable the Cisco Easy VPN remote web server interface, use the **ip http ezvpn** command in global configuration mode. To disable the Cisco Easy VPN remote web server interface, use the **no** form of this command.

Cisco uBR905 and Cisco BR925 cable access routers

ip http ezvpn

no ip http ezvpn

Syntax Description

This command has no arguments or keywords.

Defaults

The Cisco Easy VPN Remote web server interface is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(8)YJ	This command was introduced for the Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

This command enables the Cisco Easy VPN Remote web server, an onboard web server that allows users to connect an IPSec Easy VPN tunnel and to provide the required authentication information. The Cisco Easy VPN Remote web server allows the user to perform these functions without having to use the Cisco command-line interface (CLI).

Before using this command, you must first enable the Cisco web server that is onboard the cable access router by entering the **ip http server** command. Then use the **ip http ezvpn** command to enable the Cisco Easy VPN remote web server. You can then access the web server by entering the IP address for the Ethernet interface of the router in your web browser.

Note The Cisco Easy VPN Remote web interface does not work with the cable monitor web interface in Cisco IOS Release 12.2(8)YJ. To access the cable monitor web interface, you must first disable the Cisco Easy VPN remote web interface with the **no ip http ezvpn** command, and then enable the cable monitor with the **ip http cable-monitor** command.

Examples

The following example shows how to enable the Cisco Easy VPN remote web server interface:

```
Router# configure terminal
Router(config)# ip http server
Router(config)# ip http ezvpn
Router(config)# exit
Router# copy running-config startup-config
```

Related Commands

Command	Description
ip http cable-monitor	Enables and disables the Cable Monitor Web Server feature.
ip http port	Configures the TCP port number for the HTTP web server of the router.
ip http server	Enables and disables the HTTP web server of the router.

ip inspect

To apply a set of inspection rules to an interface, use the ip inspect command in interface configuration mode. There are two different modes for this command, configuration mode and interface configuration mode. To remove the set of rules from the interface, use the **no** form of this command.

Global Configuation Mode

ip inspect *inspection-name* {**in** | **out**} [**redundancy** | **stateful** *hsrp-group-name*} | **update seconds** *seconds*]

no ip inspect *inspection-name* {**in** | **out**} [**redundancy** | **stateful** *hsrp-group-name*} | **update seconds** *seconds*]

Interface Configuration Mode

ip inspect *inspection-name* {**in** | **out}** [**redundancy** | **stateful** *hsrp-group-name*]

no ip inspect *inspection-name* {**in** | **out}** [**redundancy** | **stateful** *hsrp-group-name*]

Syntax Description

Interface Configuration Mode	
inspection-name	Identifies which set of inspection rules to apply.
in	Applies the inspection rules to inbound interface.
out	Applies the inspection rules to outbound interface.
redunancy	Enables reduncany.
stateful	Enables stateful redundancy.
hsrp-group-name	The hsrp-group name that is used to configure box-to-box HA
Global Configuration Mode	
redundancy	Redundancy settings for firewall sessions
update	Update settings for firewall HA sessions
seconds *seconds*	The time interval between consecutive updates from 10 to 60 seconds. The default is 10 seconds.

Command Default

If no set of inspection rules is applied to an interface, no traffic will be inspected by CBAC. If **redundancy stateful <hsrp-grp-name>** is not used, there will be no stateful firewall high-availability.

Command Modes

Interface configuration mode(conf-if)

Command History

Release	Modification
11.2	This command was introduced.
12.4(6)T	Added support for **redunancy**, **update**, **seconds**, and **stateful** keywords.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to apply a set of inspection rules to an interface.

Typically, if the interface connects to the external network, you apply the inspection rules to outbound traffic; alternately, if the interface connects to the internal network, you apply the inspection rules to inbound traffic.

In the Interface Configuration mode, use **ip inspect<name> in/out redundancy stateful <hsrp-group>** command. Use the redundancy stateful <hsrp-grp> option to turn on stateful high availability for all session that come up on this inspect rule. The incoming IP traffic is the return traffic of an existing session. It not necessary to have redundancy stateful HSRP group name if you do not require IOS Firewall High availability.

In the Global Configuration mode, use **ip inspect redundancy update seconds <10-60>**. Use the redundancy update seconds option to configure the time interval between the synchronization of the active and standby firewall HA sessions.

Examples

The following example applies a set of inspection rules named MY-INSPECT_RULE to serial0 interface's outbound traffic. This causes the inbound IP traffic to be permitted only if the traffic is part of an existing session, and to be denied if the traffic is not part of an existing session.

```
interface serial0
ip inspect MY-INSPECT_RULE out redundancy stateful B2B-HA-HSRP-GRP
```

Related Commands

Command	Description
ip inspect name	Defines a set of inspection rules.

ip inspect alert-off

To disable Context-based Access Control (CBAC) alert messages, which are displayed on the console, use the **ip inspect alert-off** command in global configuration mode. To enable CBAC alert messages, use the **no** form of this command.

ip inspect alert-off [**vrf** *vrf-name*]

no ip inspect alert-off [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Disables CBAC alert messages only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

Alert messages are displayed.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example disables CBAC alert messages:

```
ip inspect alert-off
```

ip inspect audit trail

To turn on Context-based Access Control (CBAC) audit trail messages, which will be displayed on the console after each CBAC session closes, use the **ip inspect audit trail** command in global configuration mode. To turn off CBAC audit trail messages, use the **no** form of this command.

ip inspect audit trail [**vrf** *vrf-name*]

no ip inspect audit trail [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Turns on CBAC audit trail messages only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

Audit trail messages are not displayed.

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to turn on CBAC audit trail messages.

Examples

The following example turns on CBAC audit trail messages:

```
ip inspect audit trail
```

Afterward, audit trail messages such as the following are displayed. These messages are examples of audit trail messages. To determine which protocol was inspected, see the port number of the responder. The port number follows the IP address of the responder.

```
%FW-6-SESS_AUDIT_TRAIL: tcp session initiator (192.168.1.13:33192) sent 22 bytes --
responder (192.168.129.11:25) sent 208 bytes
%FW-6-SESS_AUDIT_TRAIL: ftp session initiator 192.168.1.13:33194) sent 336 bytes --
responder (192.168.129.11:21) sent 325 bytes
```

The following example disables CBAC alert messages for VRF interface vrf1:

```
ip inspect audit-trail vrf vrf1
```

Following are examples of audit trail messages:

```
00:10:15: %FW-6-SESS_AUDIT_TRAIL: VRF-vrf1:Stop udp session: initiator
(192.168.14.1:40801) sent 54 bytes -- responder (192.168.114.1:7) sent 54 bytes
00:10:47: %FW-6-SESS_AUDIT_TRAIL: VRF-vrf1:Stop ftp-data session: initiator
(192.168.114.1:20) sent 80000 bytes -- responder (192.168.14.1:38766) sent 0 bytes
00:10:47: %FW-6-SESS_AUDIT_TRAIL: VRF-vrf1:Stop ftp session: initiator
(192.168.14.1:38765) sent 80 bytes -- responder (192.168.114.1:21) sent 265 bytes
00:10:57: %FW-6-SESS_AUDIT_TRAIL: VRF-vrf1:Stop rcmd session: initiator (192.168.14.1:531)
sent 31 bytes -- responder (192.168.114.1:514) sent 12 bytes
00:10:57: %FW-6-SESS_AUDIT_TRAIL: VRF-vrf1:Stop rcmd-data session: initiator
(192.168.114.1:594) sent 0 bytes -- responder (192.168.14.1:530) sent 0 bytes
```

ip inspect dns-timeout

To specify the Domain Name System (DNS) idle timeout (the length of time during which a DNS name lookup session will still be managed while there is no activity), use the **ip inspect dns-timeout** command in global configuration mode. To reset the timeout to the default of 5 seconds, use the **no** form of this command.

ip inspect dns-timeout *seconds* [**vrf** *vrf-name*]

no ip inspect dns-timeout *seconds* [**vrf** *vrf-name*]

Syntax Description

seconds	Specifies the length of time in seconds, for which a DNS name lookup session will still be managed while there is no activity. The default is 5 seconds.
vrf *vrf-name*	(Optional) Specifies the DNS idle timeout only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

5 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the software detects a valid User Datagram Protocol (UDP) packet for a new DNS name lookup session, if Context-based Access Control (CBAC) inspection is configured for UDP, the software establishes state information for the new DNS session.

If the software detects no packets for the DNS session for a time period defined by the DNS idle timeout, the software will not continue to manage state information for the session.

The DNS idle timeout applies to all DNS name lookup sessions inspected by CBAC.

The DNS idle timeout value overrides the global UDP timeout. The DNS idle timeout value also enters aggressive mode and overrides any timeouts specified for specific interfaces when you define a set of inspection rules with the **ip inspect name** command.

Examples

The following example sets the DNS idle timeout to 30 seconds:

```
ip inspect dns-timeout 30
```

The following example sets the DNS idle timeout back to the default (5 seconds):

```
no ip inspect dns-timeout
```

ip inspect hashtable

To change the size of the session hash table, use the **ip inspect hashtable** command in global configuration mode. To restore the size of the session hash table to the default, use the **no** form of this command.

ip inspect hashtable *number*

no ip inspect hashtable *number*

Syntax Description

number	Size of the hash table in terms of buckets. Possible values for the hash table are 1024, 2048, 4096, and 8192; the default value is 1024.

Defaults

1024 buckets

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Use the **ip inspect hashtable** command to increase the size of the hash table when the number of concurrent sessions increases or to reduce the search time for the session. Collisions in a hash table result in poor hash function distribution because many entries are hashed into the same bucket for certain patterns of addresses. Even if a hash function distribution evenly dispenses the input across all of the buckets, a small hash table size will not scale well if there are a large number of sessions. As the number of sessions increase, the collisions increase, which increases the length of the linked lists, thereby, deteriorating the throughput performance.

Note You should increase the hash table size when the total number of sessions running through the context-based access control (CBAC) router is approximately twice the current hash size; decrease the hash table size when the total number of sessions is reduced to approximately half the current hash size. Essentially, try to maintain a 1:1 ratio between the number of sessions and the size of the hash table.

Examples

The following example shows how to change the size of the session hash table to 2048 buckets:

```
ip inspect hashtable 2048
```

ip inspect L2-transparent dhcp-passthrough

To allow a transparent firewall to forward Dynamic Host Control Protocol (DHCP) pass-through traffic, use the **ip inspect L2-transparent dhcp-passthrough** command in global configuration mode. To return to the default functionality, use the **no** form of this command.

ip inspect L2-transparent dhcp-passthrough

no ip inspect L2-transparent dhcp-passthrough

Syntax Description

This command has no arguments or keywords.

Defaults

This command is not enabled; thus, DHCP packets are forwarded or denied according to the configured access control list (ACL).

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

A transparent firewall allows a Cisco IOS Firewall (a Layer 3 device) to operate as a Layer 2 firewall in bridging mode. Thus, the firewall can exist "transparently" to a network, no longer requiring users to reconfigure their statically defined network devices.

The **ip inspect L2-transparent dhcp-passthrough** command overrides the ACL for DHCP packets; that is, DHCP packets are forwarded even if the ACL is configured to deny all IP packets. Thus, this command can be used to enable a transparent firewall to forward DHCP packets across the bridge without inspection so clients on one side of the bridge can get an IP address from a DHCP server on the opposite side of the bridge.

Examples

Allowing DHCP Pass-Through Traffic

In this example, the static IP address of the client is removed, and the address is acquired via DHCP using the **ip address dhcp** command on the interface that is connected to the transparent firewall.

```
Router# show debug

ARP:
  ARP packet debugging is on
L2 Inspection:
  INSPECT L2 firewall debugging is on
  INSPECT L2 firewall DHCP debugging is on
Router#
Router#
! Configure DHCP passthrough
Router(config)# ip insp L2-transparent dhcp-passthrough
```

```
! The DHCP discover broadcast packet arrives from the client. Since this packet is a
! broadcast (255.255.255.255), it arrives in the flood path
*Mar  1 00:35:01.299:L2FW:insp_l2_flood:input is Ethernet0 output is Ethernet1
*Mar  1 00:35:01.299:L2FW*:Src 0.0.0.0 dst 255.255.255.255 protocol udp
*Mar  1 00:35:01.299:L2FW:udp ports src 68 dst 67
*Mar  1 00:35:01.299:L2FW:src 0.0.0.0 dst 255.255.255.255
! The DHCP pass through flag is checked and the packet is allowed
*Mar  1 00:35:01.299:L2FW:DHCP packet seen. Pass-through flag allows the packet
! The packet is a broadcast packet and therefore not sent to CBAC
*Mar  1 00:35:01.299:L2FW*:Packet is broadcast or multicast.PASS
! The DHCP server 97.0.0.23 responds to the client's request
*Mar  1 00:35:01.303:L2FW:insp_l2_flood:input is Ethernet1 output is Ethernet0
*Mar  1 00:35:01.303:L2FW*:Src 172.16.0.23 dst 255.255.255.255 protocol udp
*Mar  1 00:35:01.307:L2FW:udp ports src 67 dst 68
*Mar  1 00:35:01.307:L2FW:src 172.16.0.23 dst 255.255.255.255
*Mar  1 00:35:01.307:L2FW:DHCP packet seen. Pass-through flag allows the packet
*Mar  1 00:35:01.307:L2FW*:Packet is broadcast or multicast.PASS
*Mar  1 00:35:01.311:L2FW:insp_l2_flood:input is Ethernet0 output is Ethernet1
*Mar  1 00:35:01.311:L2FW*:Src 0.0.0.0 dst 255.255.255.255 protocol udp
*Mar  1 00:35:01.311:L2FW:udp ports src 68 dst 67
*Mar  1 00:35:01.311:L2FW:src 0.0.0.0 dst 255.255.255.255
*Mar  1 00:35:01.315:L2FW:DHCP packet seen. Pass-through flag allows the packet
*Mar  1 00:35:01.315:L2FW*:Packet is broadcast or multicast.PASS
*Mar  1 00:35:01.315:L2FW:insp_l2_flood:input is Ethernet1 output is Ethernet0
*Mar  1 00:35:01.323:L2FW*:Src 172.16.0.23 dst 255.255.255.255 protocol udp
*Mar  1 00:35:01.323:L2FW:udp ports src 67 dst 68
*Mar  1 00:35:01.323:L2FW:src 172.16.0.23 dst 255.255.255.255
*Mar  1 00:35:01.323:L2FW:DHCP packet seen. Pass-through flag allows the packet
*Mar  1 00:35:01.323:L2FW*:Packet is broadcast or multicast.PASS
! The client has an IP address (172.16.0.5) and has issued a G-ARP to let everyone know
it's address
*Mar  1 00:35:01.327:IP ARP:rcvd rep src 172.16.0.5 0008.a3b6.b603, dst 172.16.0.5 BVI1
Router#
```

Denying DHCP Pass-Through Traffic

In this example, DHCP pass-through traffic is not allowed (via the **no ip inspect L2-transparent dhcp-passthrough** command). The client is denied when it attempts to acquire a DHCP address from the server.

```
! Deny DHCP pass-through traffic
Router(config)# no ip inspect L2-transparent dhcp-passthrough

! The DHCP discover broadcast packet arrives from the client
*Mar  1 00:36:40.003:L2FW:insp_l2_flood:input is Ethernet0 output is Ethernet1
*Mar  1 00:36:40.003:L2FW*:Src 0.0.0.0 dst 255.255.255.255 protocol udp
*Mar  1 00:36:40.003:L2FW:udp ports src 68 dst 67
*Mar  1 00:36:40.007:L2FW:src 0.0.0.0 dst 255.255.255.255
! The pass-through flag is checked
*Mar  1 00:36:40.007:L2FW:DHCP packet seen. Pass-through flag denies the packet
! The packet is dropped because the flag does not allow DHCP passthrough traffic. Thus,
! the client cannot acquire an address, and it times out
*Mar  1 00:36:40.007:L2FW:FLOOD Dropping the packet after ACL check.
```

Related Commands

Command	Description
debug ip inspect L2-transparent	Enables debugging messages for transparent firewall events.
show ip inspect	Displays Cisco IOS Firewall configuration and session information.

ip inspect log drop-pkt

To log all packets dropped by the firewall, use the **ip inspect log drop-pkt** command in global configuration mode. To return to the default state, use the **no** form of this command.

ip inspect log drop-pkt

no ip inspect log drop-pkt

Syntax Description

This command has no arguments or keywords.

Command Default

Packets dropped by the firewall are not logged.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)T1	This command was introduced.
12.3(8)T	This command was integrated into Release 12.3(8)T.

Usage Guidelines

To see the packets that are dropped by the firewall, the **ip inspect log drop-pkt** command must be enabled.

Examples

The following example shows how to enable the logging of packets dropped by the firewall:

```
Router> enable
Router# configure terminal
Router(config)# ip inspect log drop-pkt
```

The following example shows a possible message that can be displayed when packets are dropped:

```
*Sep 9 19:56:28.699: %FW-6-DROP_PKT: Dropping tcp pkt 17.2.2.1:0 => 19.2.2.1:0 with ip
ident 229 due to Invalid Header length

*Sep 9 20:30:47.839: %FW-6-DROP_TCP_PKT: Dropping tcp pkt 17.2.2.1:42829 => 19.2.2.1:80
due to SYN pkt with illegal flags -- ip ident 23915 tcpflags 40962 seq.no 3928613134 ack 0

*Sep 10 00:30:24.931: %FW-6-DROP_TCP_PKT: Dropping tcp pkt 17.2.2.1:45771 =>

19.2.2.1:80 due to SYN with data or with PSH/URG flags -- ip ident 55001 tcpflags 40962
seq.no 2232798685 ack 0

*Aug 29 21:57:16.895: %FW-6-DROP_PKT: Dropping tcp pkt 17.2.2.1:51613 => 19.2.2.1:80 due
to Out-Of-Order Segment
```

Table 35 describes messages that occur when packets are dropped.

Table 35 ip inspect log drop-pkt Messages

Field	Description
Invalid Header length	The datagram is so small that it could not contain the layer 4 TCP, Universal Computer Protocol (UCP), or Internet Control Message Protocol (ICMP) header.
Police rate limiting	Rate limiting is enabled, and the packet in question has exceeded the rate limit.
Session limiting	Session limiting is on, and the session count exceeds the configured session threshold.
Bidirectional traffic disabled	Session is unidirectional and the firewall is seeing packets in the other direction and dropping the session.
SYN with data or with PSH/URG flags	TCP SYN packet is seen with data.
Segment matching no TCP connection	Non-initial TCP segment is received without a valid session.
Invalid Segment	There is an invalid TCP segment.
Invalid Seq#	The packet contains an invalid TCP sequence number.
Invalid Ack (or no Ack)	The packet contains an invalid TCP acknowledgement number.
Invalid Flags	Flags in a TCP segment are invalid.
Invalid Checksum	There is an invalid TCP checksum.
SYN inside current window	A synchronization packet is seen within the window of an already established TCP connection.
RST inside current window	A reset (RST) packet is observed within the window of an already established TCP connection.
Out-Of-Order Segment	The packets in a segment are out of order.
Retransmitted Segment with Invalid Flags	A retransmitted packet was already acknowledged by the receiver.
Stray Segment	A TCP segment is received that should not have been received through the TCP state machine such as a TCP SYN packet being received in the listen state.
Internal Error	The TCP state machine that is maintained by the firewall encounters an internal error.
Invalid Window scale option	The responder on one side of a firewall proposes an illegal window scale option. The window scale option is illegal in this case because the initiating side did not propose the option first.
Invalid TCP options	The options in the TCP header are not TCP protocol compliant.

Related Commands

Command	Description
ip inspect tcp block-non-session	Blocks packets that do not belong to the existing firewall TCP sessions in the inbound and outbound directions.
ip inspect tcp finwait-time	Defines how long a TCP session will still be managed after the firewall detects a FIN-exchange.
ip inspect tcp idle-time	Specifies the TCP idle timeout (the length of time a TCP session will still be managed while there is no activity).
ip inspect tcp max-incomplete host	Specifies threshold and blocking time values for TCP host-specific DoS detection and prevention.
ip inspect tcp reassembly	Sets parameters that define how Cisco IOS Firewall application inspection and Cisco IOS IPS will handle out-of-order TCP packets.
ip inspect tcp synwait-time	Defines how long the software will wait for a TCP session to reach the established state before dropping the session.
ip inspect udp idle-time	Specifies the UDP idle timeout (the length of time for which a UDP session will still be managed while there is no activity).

ip inspect max-incomplete high

To define the number of existing half-open sessions that will cause the software to start deleting half-open sessions, use the **ip inspect max-incomplete high** command in global configuration mode. To reset the threshold to the default of 500 half-open sessions, use the **no** form of this command.

ip inspect max-incomplete high *number* [**vrf** *vrf-name*]

no ip inspect max-incomplete high

Syntax Description

number	Specifies the number of existing half-open sessions that will cause the software to start deleting half-open sessions. The default is 500 half-open sessions.
vrf *vrf-name*	(Optional) Defines the number of existing half-open sessions only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

500 half-open sessions

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, “half-open” means that the session has not reached the established state. For User Datagram Protocol (UDP), “half-open” means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (the **max-incomplete high** number), the software will delete half-open sessions as required to accommodate new connection requests. The software will continue to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (the **max-incomplete low** number).

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Examples

The following example causes the software to start deleting half-open sessions when the number of existing half-open sessions rises above 900, and to stop deleting half-open sessions when the number drops below 800:

```
ip inspect max-incomplete high 900
ip inspect max-incomplete low 800
```

The following example shows an ALERT_ON message generated for the **ip inspect max-incomplete high** command:

```
ip inspect max-incomplete high 20 vrf vrf1
show log / include ALERT_ON
00:59:00:%FW-4-ALERT_ON: VRF-vrf1:getting aggressive, count (21/20) current 1-min rate: 21
```

Related Commands

Command	Description
ip inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ip inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ip inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.
ip inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific DoS detection and prevention.

ip inspect max-incomplete low

To define the number of existing half-open sessions that will cause the software to stop deleting half-open sessions, use the **ip inspect max-incomplete low** command in global configuration mode. To reset the threshold to the default of 400 half-open sessions, use the **no** form of this command.

ip inspect max-incomplete low *number* [**vrf** *vrf-name*]

no ip inspect max-incomplete low

Syntax Description

number	Specifies the number of existing half-open sessions that will cause the software to stop deleting half-open sessions. The default is 400 half-open sessions.
vrf *vrf-name*	(Optional) Defines the number of existing half-open sessions only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

400 half-open sessions

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, “half-open” means that the session has not reached the established state. For User Datagram Protocol (UDP), “half-open” means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (the **max-incomplete high** number), the software will delete half-open sessions as required to accommodate new connection requests. The software will continue to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (the **max-incomplete low** number).

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Examples

The following example causes the software to start deleting half-open sessions when the number of existing half-open sessions rises above 900, and to stop deleting half-open sessions when the number drops below 800:

```
ip inspect max-incomplete high 900
ip inspect max-incomplete low 800
```

The following example shows an ALERT_OFF message generated for the **ip inspect max-incomplete low** command:

```
ip inspect max-incomplete low 10 vrf vrf1
show log / include ALERT_OFF
00:59:31: %FW-4-ALERT_OFF: VRF-vrf1:calming down, count (9/10) current 1-min rate: 100
```

Related Commands

Command	Description
ip inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ip inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ip inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.
ip inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific DoS detection and prevention.

ip inspect name

To define a set of inspection rules, use the **ip inspect name** command in global configuration mode. To remove the inspection rule for a protocol or to remove the entire set of inspection rules, use the **no** form of this command.

ip inspect name *inspection-name* [**parameter max-sessions** *number*] *protocol* [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**timeout** *seconds*]

no ip inspect name *inspection-name* [**parameter max-sessions** *number*] *protocol* [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**timeout** *seconds*]

HTTP Inspection Syntax

ip inspect name *inspection-name* **http** [**java-list** *access-list*] [**urlfilter**] [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**timeout** *seconds*]

no ip inspect name *inspection-name protocol*

Simple Mail Transfer Protocol (SMTP) and Extended SMTP Inspection (ESMTP) Syntax

ip inspect name *inspection-name* {**smtp** | **esmtp**} [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**max-data** *number*] [**timeout** *seconds*]

remote-procedure call (RPC) Inspection Syntax

ip inspect name *inspection-name* [**parameter max-sessions** *number*] **rpc program-number** *number* [**wait-time** *minutes*] [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**timeout** *seconds*]

no ip inspect name *inspection-name protocol*

Post Office Protocol 3(POP3)/ Internet Message Access Protocol(IMAP) Inspection Syntax

ip inspect name *inspection-name* **imap** [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**reset**] [**secure-login**] [**timeout** *number*]

ip inspect name *inspection-name* **pop3** [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**reset**] [**secure-login**] [**timeout** *number*]

Fragment Inspection Syntax

ip inspect name *inspection-name* [**parameter max-sessions** *number*] **fragment** [**max** *number* **timeout** *seconds*]

no ip inspect name *inspection-name* [**parameter max-sessions** *number*] **fragment** [**max** *number* **timeout** *seconds*]

Application Firewall Provisioning Syntax

ip inspect name *inspection-name* [**parameter max-sessions** *number*] **appfw** *policy-name*

no ip inspect name *inspection-name* [**parameter max-sessions** *number*] **appfw** *policy-name*

User-Defined Application Syntax

ip inspect name *inspection-name user-10* [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**timeout** *seconds*}

no ip inspect name *inspection-name user-10* [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**timeout** *seconds*}

Session Limiting Syntax

no ip inspect name *inspection-name* [**parameter max-sessions** *number*]

Syntax Description

inspection-name	Name the set of inspection rules. If you want to add a protocol to an existing set of rules, use the same *inspection-name* as the existing set of rules. **Note** The *inspection-name* cannot exceed 16 characters; otherwise, the name will be truncated to the 16-character limit.
parameter max-sessions *number*	(Optional) Limits the number of established firewall sessions that a firewall rule creates. By default, there is no limit to the number of firewall sessions.
protocol	A protocol keyword listed in Table 36 or Table 37.
alert {**on** | **off**}	(Optional) For each inspected protocol, the generation of alert messages can be set be **on** or **off**. If no option is selected, alerts are generated on the basis of the setting of the **ip inspect alert-off** command.
audit-trail {**on** | **off**}	(Optional) For each inspected protocol, **audit trail** can be set **on** or **off**. If no option is selected, an audit trail message is generated depending on the configuration of the **ip inspect audit-trail** command.
timeout *seconds*	(Optional) To override the global TCP or UDP, or Internet Control Message Protocol (ICMP) idle timeouts for the specified protocol, specify the number of seconds for a different idle timeout. This timeout overrides the global TCP, UDP, or ICMP timeouts but will not override the global Domain Name System (DNS) timeout.
http	Specifies the HTTP protocol for Java applet blocking.
java-list *access-list*	(Optional) Specifies the numbered standard access list to use to determine “friendly” sites. This keyword is available only for the HTTP protocol, for Java applet blocking. Java blocking works only with numbered standard access lists.
urlfilter	(Optional) Associates URL filtering with HTTP inspection.
smtp | **esmtp**	Specifies the protocol being used to inspect the traffic.
max-data *number*	(Optional) Specifies the maximum amount of data, in bytes, that can be transferred in a single Simple Mail Transport Protocol (SMTP) session. After the maximum value is exceeded, the firewall logs an alert message and closes the session. The default value is 20MB.
rpc program-number *number*	Specifies the program number to permit. This keyword is available only for the remote-procedure call (RPC) protocol.

wait-time *minutes*	(Optional) Specifies the number of minutes to keep a small gap in the firewall to allow subsequent connections from the same source address and to the same destination address and port. The default wait-time is zero minutes. This keyword is available only for the RPC protocol.
imap	Specifies that the Internet Message Access Protocol (IMAP) is being used.
reset	(Optional) Resets the TCP connection if the client enters a nonprotocol command before authentication is complete.
secure-login	(Optional) Causes a user at a nonsecure location to use encryption for authentication.
pop3	Specifies that the Post Office Protocol, Version 3 (POP3) is being used.
fragment	Specifies fragment inspection for the named rule.
max *number*	(Optional) Specifies the maximum number of unassembled packets for which state information (structures) is allocated by Cisco IOS software. Unassembled packets are packets that arrive at the router interface before the initial packet for a session. The acceptable range is 50 through 10000. The default is 256 state entries. • Memory is allocated for the state structures, and setting this value to a larger number may cause memory resources to be exhausted.
timeout *seconds* (fragmentation)	(Optional) Configures the number of seconds that a packet state structure remains active. When the timeout value expires, the router drops the unassembled packet, freeing that structure for use by another packet. The default timeout value is 1 second. • If this number is set to a value greater that 1 second, it is automatically adjusted by the Cisco IOS software when the number of free state structures goes below certain thresholds: when the number of free states is fewer than 32, the timeout is divided by 2. When the number of free states is fewer than 16, the timeout is set to 1 second.
appfw	Specifies application firewall provisioning.
policy-name	Application firewall policy name. **Note** This name must match the name specified via the **appfw policy-name** command.

Command Default No inspection rules are defined.

Command Modes Global configuration (config)

Command History

Release	Modification
11.2P	This command was introduced.
12.0(5)T	This command was modified. Support was added for configurable alert and audit trail, IP fragmentation checking, and NetShow protocol.
12.2(11)YU	This command was modified. Support was added for ICMP and Session Initiation Protocol (SIP) protocols. The **urlfilter** keyword was added to the HTTP inspection syntax.
12.2(15)T	This command was modified. Support was added for ICMP, SIP, and the **urlfilter** keyword was added.
12.3(1)	This command was modified. Skinny protocol support was added.
12.3(7)T	This command was modified. Extended Simple Mail Transfer Protocol (ESMTP) protocol support was added.
12.3(14)T	This command was modified. The **appfw** keyword and the *policy-name* argument were added to support application firewall provisioning. The **parameter max-sessions**, **reset**, **router-traffic,** and **secure-login**, and keywords were added. Support for a larger list of protocols including user-defined applications was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(1)T	This command was modified. Support for the CU-SeeMe protocol and the **cuseeme** keyword was removed.

Usage Guidelines

To define a set of inspection rules, enter the **ip inspect name** command for each protocol that you want the Cisco IOS firewall to inspect, using the same *inspection-name*. Give each set of inspection rules a unique *inspection-name*, which should not exceed the 16-character length limit. Define either one or two sets of rules per interface—you can define one set to examine both inbound and outbound traffic, or you can define two sets: one for outbound traffic and one for inbound traffic. The **no ip inspect-name** *protocol* removes the inspection rule for the specified protocol.

no ip inspect name command removes the entire set of inspection rules.

To define a single set of inspection rules, configure inspection for all the desired application-layer protocols, and for ICMP, TCP, and UDP, or as desired. This combination of TCP, UDP, and application-layer protocols join together to form a single set of inspection rules with a unique name. (There are no application-layer protocols associated with ICMP.)

To remove the inspection rule for a protocol, use the **no** form of this command with the specified inspection name and protocol; To remove the entire set of inspection rules, use the **no** form of this command only; that is, do not list any inspection names or protocols.

In general, when inspection is configured for a protocol, return traffic entering the internal network will be permitted only if the packets are part of a valid, existing session for which state information is being maintained.

Table 36 Protocol Keywords—Transport-Layer and Network-Layer Protocols

Protocol	Keyword
ICMP	**icmp**
TCP	**tcp**
UDP	**udp**

Note The TCP, UDP, and H.323 protocols support the **router-traffic** keyword, which enables inspection of traffic destined to or originated from a router. The command format is as follows:

ip inspect name *inspection-nam*e {**tcp** | **udp** | **H323**} [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**router-traffic**][**timeout** *seconds*]

TCP and UDP Inspection

You can configure TCP and UDP inspection to permit TCP and UDP packets to enter the internal network through the firewall, even if the application-layer protocol is not configured to be inspected. However, TCP and UDP inspection do not recognize application-specific commands, and therefore might not permit all return packets for an application, particularly if the return packets have a different port number from the previous exiting packet.

Any application-layer protocol that is inspected will take precedence over the TCP or UDP packet inspection. For example, if inspection is configured for FTP, all control channel information will be recorded in the state table, and all FTP traffic will be permitted back through the firewall if the control channel information is valid for the state of the FTP session. The fact that TCP inspection is configured is irrelevant.

With TCP and UDP inspection, packets entering the network must exactly match an existing session. The entering packets must have the same source or destination addresses and source or destination port numbers as the exiting packet (but reversed). Otherwise, the entering packets will be blocked at the interface.

Granular protocol inspection allows you to specify TCP or UDP ports by using the port-to-application mapping (PAM) table. This eliminates having to inspect all applications running under TCP or UDP and the need for multiple ACLs to filter the traffic.

Using the PAM table, you can pick an existing application or define a new one for inspection, thereby simplifying Access Control List (ACL) configuration.

ICMP Inspection

ICMP inspection sessions are done on the basis of the source address of the inside host that originates the ICMP packet. Dynamic ACLs are created for return ICMP packets of the allowed types (echo-reply,destination unreachable, time-exceeded, and timestamp reply) for each session. No port numbers associated with an ICMP session, and the permitted IP address of the return packet is a wild-card in the ACL. The wildcard address is because the IP address of the return packet cannot be known in advance for time-exceeded and destination-unreachable replies. These replies can come from intermediate devices rather than the intended destination.

Application-Layer Protocol Inspection

In general, if you configure inspection for an application-layer protocol, packets for that protocol should be permitted to exit the firewall (by configuring the correct ACL), and packets for that protocol will be allowed back in through the firewall only if they belong to a valid existing session. Each protocol packet is inspected to maintain information about the session state.

Java, H.323, RPC, SIP, and SMTP inspection have additional information, described in the next five sections. Table 37 lists the supported application-layer protocols.

Table 37 Protocol Keywords—Application-Layer Protocols

Protocol	Keyword
Application Firewall	**appfw**
CU-SeeMe	**cuseeme**
ESMTP	**smtp**
FTP	**ftp**
IMAP	**imap**
Java	**http**
H.323	**h323**
Microsoft NetShow	**netshow**
POP3	**pop3**
RealAudio	**realaudio**
RPC	**rpc**
SIP	**sip**
Simple Mail Transfer Protocol (SMTP)	**smtp**
Skinny Client Control Protocol (SCCP)	**skinny**
StreamWorks	**streamworks**
Structured Query Language*Net (SQL*Net)	**sqlnet**
TFTP	**tftp**
UNIX R commands (rlogin, rexec, rsh)	**rcmd**
VDOLive	**vdolive**
WORD	**user-defined application name**; **use prefix -user** **Note** All applications that appear under the **show ip port-map** command are supported.

Java Inspection

Java inspection enables Java applet filtering at the firewall. Java applet filtering distinguishes between trusted and untrusted applets by relying on a list of external sites that you designate as “friendly.” If an applet is from a friendly site, the firewall allows the applet through. If the applet is not from a friendly site, the applet will be blocked. Alternately, you could permit applets from all sites except sites specifically designated as “hostile.”

Note Before you configure Java inspection, you must configure a numbered standard access list that defines "friendly" and "hostile" external sites. You configure this numbered standard access list to permit traffic from friendly sites, and to deny traffic from hostile sites. If you do not configure a numbered standard access list, but use a "placeholder" access list in the **ip inspect name** *inspection-name* **http** command, all Java applets will be blocked.

Note Java blocking forces a strict order on TCP packets. To properly verify that Java applets are not in the response, a firewall will drop any TCP packet that is out of order. Because the network—not the firewall—determines how packets are routed, the firewall cannot control the order of the packets; the firewall can only drop and retransmit all TCP packets that are not in order.

Caution Context-Based Access Control (CBAC) does not detect or block encapsulated Java applets. Therefore, Java applets that are wrapped or encapsulated, such as applets in .zip or .jar format, are *not* blocked at the firewall. CBAC also does not detect or block applets loaded via FTP, gopher, or HTTP on a nonstandard port.

H.323 Inspection

If you want CBAC inspection to work with NetMeeting 2.0 traffic (an H.323 application-layer protocol), you must also configure inspection for TCP, as described in the chapter "Configuring Context-Based Access Control" in the *Cisco IOS Security Configuration Guide*. This requirement exists because NetMeeting 2.0 uses an additional TCP channel not defined in the H.323 specification.

RPC Inspection

RPC inspection allows the specification of various program numbers. You can define multiple program numbers by creating multiple entries for RPC inspection, each with a different program number. If a program number is specified, all traffic for that program number will be permitted. If a program number is not specified, all traffic for that program number will be blocked. For example, if you created an RPC entry with the NFS program number, all NFS traffic will be allowed through the firewall.

SIP Inspection

You can configure SIP inspection to permit media sessions associated with SIP-signaled calls to traverse the firewall. Because SIP is frequently used to signal both incoming and outgoing calls, it is often necessary to configure SIP inspection in both directions on a firewall (both from the protected internal network and from the external network). Because inspection of traffic from the external network is not done with most protocols, it may be necessary to create an additional inspection rule to cause only SIP inspection to be performed on traffic coming from the external network.

SMTP Inspection

SMTP inspection causes SMTP commands to be inspected for illegal commands. Packets with illegal commands are modified to a "xxxx" pattern and forwarded to the server. This process causes the server to send a negative reply, forcing the client to issue a valid command. An illegal SMTP command is any command except the following:

- DATA
- HELO
- HELP

- MAIL
- NOOP
- QUIT
- RCPT
- RSET
- SAML
- SEND
- SOML
- VRFY

ESMTP Inspection

Like SMTP, ESMTP inspection also causes the commands to be inspected for illegal commands. Packets with illegal commands are modified to a "xxxx" pattern and forwarded to the server. This process causes the server to send a negative reply, forcing the client to issue a valid command. An illegal ESMTP command is any command except the following:

- AUTH
- DATA
- EHLO
- ETRN
- HELO
- HELP
- MAIL
- NOOP
- QUIT
- RCPT
- RSET
- SAML
- SEND
- SOML
- VRFY

In addition to inspecting commands, the ESMTP firewall also inspects the following extensions via deeper command inspection:

- Message Size Declaration (SIZE)
- Remote Queue Processing Declaration (ETRN)
- Binary MIME (BINARYMIME)
- Command Pipelining
- Authentication
- Delivery Status Notification (DSN)

- Enhanced Status Code (ENHANCEDSTATUSCODE)
- 8bit-MIMEtransport (8BITMIME)

Note SMTP and ESMTP cannot exist simultaneously. An attempt to configure both protocols will result in an error message.

Use of the urlfilter Keyword

If you specify the **urlfilter** keyword, the Cisco IOS Firewall will interact with a URL filtering software to control web traffic for a given host or user on the basis of a specified security policy.

Note Enabling HTTP inspection with or without any option triggers the Java applet scanner, which is CPU intensive. The only way to stop the Java applet scanner is to specify the **java-list** *access-list* option. Configuring URL filtering without enabling the **java-list** *access-list* option will severely impact performance.

Use of the timeout Keyword

If you specify a timeout for any of the transport-layer or application-layer protocols, the timeout will override the global idle timeout for the interface to which the set of inspection rules is applied.

If the protocol is TCP or a TCP application-layer protocol, the timeout will override the global TCP idle timeout. If the protocol is UDP or a UDP application-layer protocol, the timeout will override the global UDP idle timeout.

If you do not specify a timeout for a protocol, the timeout value applied to a new session of that protocol will be taken from the corresponding TCP or UDP global timeout value valid at the time of session creation.

The default ICMP timeout is deliberately short (10 seconds) due to the security hole that is opened by allowing ICMP packets with a wild-card source address back into the inside network. The timeout will occur 10 seconds after the last outgoing packet from the originating host. For example, if you send a set of 10 ping packets spaced one second apart, the timeout will expire in 20 seconds or 10 seconds after the last outgoing packet. However, the timeout is not extended for return packets. If a return packet is not seen within the timeout window, the gap will be closed and the return packet will not be allowed in. Although the default timeout can be made longer if desired, it is recommended that this value be kept relatively short.

IP Fragmentation Inspection

CBAC inspection rules can help protect hosts against certain denial-of-service attacks involving fragmented IP packets. Even though the firewall keeps an attacker from making actual connections to a given host, the attacker may still be able to disrupt services provided by that host. This is done by sending many noninitial IP fragments or by sending complete fragmented packets through a router with an ACL that filters the first fragment of a fragmented packet. These fragments can tie up resources on the target host as it tries to reassemble the incomplete packets.

Using fragmentation inspection, the firewall maintains an *interfragment state* (structure) for IP traffic. Noninitial fragments are discarded unless the corresponding initial fragment was permitted to pass through the firewall. Noninitial fragments received before the corresponding initial fragments are discarded.

Note Fragmentation inspection can have undesirable effects in certain cases, because it can result in the firewall discarding any packet whose fragments arrive out of order. There are many circumstances that can cause out-of-order delivery of legitimate fragments. Apply fragmentation inspection in situations where legitimate fragments, which are likely to arrive out of order, might have a severe performance impact.

Because routers running Cisco IOS software are used in a very large variety of networks, and because the CBAC feature is often used to isolate parts of internal networks from one another, the fragmentation inspection feature is not enabled by default. Fragmentation detection must be explicitly enabled for an inspection rule using the **ip inspect name** command. Unfragmented traffic is never discarded because it lacks a fragment state. Even when the system is under heavy attack with fragmented packets, legitimate fragmented traffic, if any, will still get some fraction of the firewall's fragment state resources, and legitimate, unfragmented traffic can flow through the firewall unimpeded.

Application Firewall Provisioning

Application firewall provisioning allows you to configure your Cisco IOS Firewall to detect and prohibit a specific protocol type of traffic.

Most firewalls provide packet filtering capabilities that simply permit or deny traffic without inspecting the data stream; the Cisco IOS application firewall can detect whether a packet is in compliance with a given HTTP protocol. If the packet is determined to be unauthorized, it will be dropped, the connection will be reset, and a syslog message will be generated, as appropriate.

User-Defined Applications

You can define your own applications and enter them into the PAM table using the **ip port-map** command. Then you set up your inspection rules by inserting your user-defined application as a value for the *protocol* argument in the **ip inspect name** command.

Session Limiting

Users can limit the number of established firewall sessions that a firewall rule creates by setting the "max-sessions" threshold. A session counter is maintained for each firewall interface. When a session count exceeds the specified threshold, an alert FW-4-SESSION_THRESHOLD_EXCEEDED message is logged to the syslog server and no new sessions can be created.

Examples

The following example causes the software to inspect TCP sessions and UDP sessions, and to specifically allow CU-SeeMe, FTP, and RPC traffic back through the firewall for existing sessions only. For UDP traffic, audit-trail is on. For FTP traffic, the idle timeout is set to override the global TCP idle timeout. For RPC traffic, program numbers 100003, 100005, and 100021 are permitted.

```
ip inspect name myrules tcp
ip inspect name myrules udp audit-trail on
ip inspect name myrules cuseeme
ip inspect name myrules ftp timeout 120
ip inspect name myrules rpc program-number 100003
ip inspect name myrules rpc program-number 100005
ip inspect name myrules rpc program-number 100021
```

The following example adds fragment checking to software inspection of TCP and UDP sessions for the rule named "myrules." In this example, the firewall software will allocate 100 state structures, and the timeout value for dropping unassembled packets is set to 4 seconds. If 100 initial fragments for 100 different packets are sent through the router, all of the state structures will be used up. The initial

fragment for packet 101 will be dropped. Additionally, if the number of free state structures (structures available for use by unassembled packets) drops below the threshold values, 32 or 16, the timeout value is automatically reduced to 2 or 1, respectively. Changing the timeout value frees up packet state structures more quickly.

```
ip inspect name myrules tcp
ip inspect name myrules udp audit-trail on
ip inspect name myrules cuseeme
ip inspect name myrules ftp timeout 120
ip inspect name myrules rpc program-number 100003
ip inspect name myrules rpc program-number 100005
ip inspect name myrules rpc program-number 100021
ip inspect name myrules fragment max 100 timeout 4
```

The following firewall and SIP example shows how to allow outside-initiated calls and internal calls. For outside-initiated calls, an ACL needs to be accessed to allow for the traffic from the initial signaling packet from outside. Subsequent signaling and media channels will be allowed by the inspection module.

```
ip inspect name voip sip
interface FastEthernet0/0
 ip inspect voip in
!
!
interface FastEthernet0/1
 ip inspect voip in
 ip access-group 100 in
!
!
access-list 100 permit udp host <gw ip> any eq 5060
access-list 100 permit udp host <proxy ip> any eq 5060
access-list deny ip any any
```

The following example shows two configured inspections named fw_only and fw_urlf; URL filtering will work only on the traffic that is inspected by fw_urlf. Note that the **java-list** *access-list* option has been enabled, which disables java scanning.

```
ip inspect name fw_only http java-list 51 timeout 30
interface e0
 ip inspect fw_only in
!
ip inspect name fw_urlf  http java-list 51 urlfilter timeout 30
interface e1
 ip inspect fw_urlf in
```

The following example shows how to define the HTTP application firewall policy mypolicy. This policy includes all supported HTTP policy rules. This example also includes sample output from the **show appfw configuration** and **show ip inspect config** commands, which allow you to verify the configured setting for the application policy.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
```

```
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
! Issue the show appfw configuration command and the show ip inspect config command after
the inspection rule "mypolicy" is applied to all incoming HTTP traffic on the
FastEthernet0/0 interface.
!
Router# show appfw configuration

Application Firewall Rule configuration
  Application Policy name mypolicy
    Application http
      strict-http action allow alarm
      content-length minimum 0 maximum 1 action allow alarm
      content-type-verification match-req-rsp action allow alarm
      max-header-length request length 1 response length 1 action allow alarm
      max-uri-length 1 action allow alarm
      port-misuse default action allow alarm
      request-method rfc default action allow alarm
      request-method extension default action allow alarm
      transfer-encoding default action allow alarm

Router# show ip inspect config

Session audit trail is disabled
Session alert is enabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
Inspection name firewall
http alert is on audit-trail is off timeout 3600
```

Related Commands

Command	Description
ip inspect	Applies a set of inspection rules to an interface.
ip inspect alert-off	Disables CBAC alert messages.
ip inspect audit trail	Turns on CBAC audit trail messages, which will be displayed on the console after each CBAC session close.

ip inspect one-minute high

To define the rate of new unestablished sessions that will cause the software to start deleting half-open sessions, use the **ip inspect one-minute high** command in global configuration mode. To reset the threshold to the default of 500 half-open sessions, use the **no** form of this command.

i**p inspect one-minute high** *number* [**vrf** *vrf-name*]

no ip inspect one-minute high

Syntax Description

number	Specifies the rate of new unestablished TCP sessions that will cause the software to start deleting half-open sessions. The default is 500 half-open sessions.
vrf *vrf-name*	(Optional) Defines the information only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

500 half-open sessions

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, “half-open” means that the session has not reached the established state. For User Datagram Protocol (UDP), “half-open” means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are included in the total number and rate measurements. Measurements are made once a minute.

When the rate of new connection attempts rises above a threshold (the **one-minute high** number), the software will delete half-open sessions as required to accommodate new connection attempts. The software will continue to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (the **one-minute low** number). The rate thresholds are measured as the number of new session connection attempts detected in the last one-minute sample period. (The rate is calculated as an exponentially decayed rate.)

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Examples

The following example causes the software to start deleting half-open sessions when more than 1000 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 950 session establishment attempts have been detected in the last minute:

```
ip inspect one-minute high 1000
ip inspect one-minute low 950
```

Related Commands

Command	Description
ip inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.
ip inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ip inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ip inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific DoS detection and prevention.

ip inspect one-minute low

To define the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions, use the **ip inspect one-minute low** command in global configuration mode. To reset the threshold to the default of 400 half-open sessions, use the **no** form of this command.

ip inspect one-minute low *number* [**vrf** *vrf-name*]

no ip inspect one-minute low

Syntax Description

number	Specifies the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions. The default is 400 half-open sessions.
vrf *vrf-name*	(Optional) Defines the information only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

400 half-open sessions

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, “half-open” means that the session has not reached the established state. For User Datagram Protocol (UDP), “half-open” means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are included in the total number and rate measurements. Measurements are made once a minute.

When the rate of new connection attempts rises above a threshold (the **one-minute high** number), the software will delete half-open sessions as required to accommodate new connection attempts. The software will continue to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (the **one-minute low** number). The rate thresholds are measured as the number of new session connection attempts detected in the last one-minute sample period. (The rate is calculated as an exponentially decayed rate.)

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Examples

The following example causes the software to start deleting half-open sessions when more than 1000 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 950 session establishment attempts have been detected in the last minute:

```
ip inspect one-minute high 1000
ip inspect one-minute low 950
```

Related Commands

Command	Description
ip inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ip inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ip inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ip inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific DoS detection and prevention.

ip inspect tcp block-non-session

To block packets that do not belong to the existing firewall TCP sessions in the inbound and outbound directions, use the **ip inspect tcp block-non-session** command in global configuration mode. To return to the default state, use the **no** form of this command.

ip inspect tcp block-non-session [**vrf** *vrf-name*]

no inspect tcp block-non-session [**vrf** *vrf-name*]

Syntax Description

vrf	(Optional) Declares a specific VPN routing/forwarding instance (VRF).
vrf-name	(Optional) Name of the VRF.

Command Default

TCP packets that do not belong to an existing TCP session on the firewall are allowed through the firewall.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(6)	This command was introduced.
12.3(7)T	This command was integrated into Release 12.3(6)T.
12.3(7)XI	This command was integrated into the Release 12.3(7)XI.
12.3(14)T	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

This command will deny TCP packets that do not belong to an existing TCP session the firewall knows about. To be applicable, the following conditions must be met:

- The TCP packets should traverse interfaces where a firewall rule is applicable.
- The TCP packets should be non-connection initiating (that is, packets without the SYN bit set in them). For connection initiating packets, the existing rules of session creation would apply.

Examples

The following example shows how to configure the firewall to block any externally initiated TCP sessions:

```
Router> enable
Router# config terminal
Router(config)# ip inspect tcp block-non-session
```

Related Commands

Command	Description
ip inspect log drop-pkt	Logs all packets dropped by the firewall.
ip inspect tcp finwait-time	Defines how long a TCP session will still be managed after the firewall detects a FIN-exchange.
ip inspect tcp idle-time	Specifies the TCP idle timeout (the length of time a TCP session will still be managed while there is no activity).
ip inspect tcp max-incomplete host	Specifies threshold and blocking time values for TCP host-specific (DoS) detection and prevention.
ip inspect tcp reassembly	Sets parameters that define how Cisco IOS Firewall application inspection and Cisco IOS IPS will handle out-of-order TCP packets.
ip inspect tcp synwait-time	Defines how long the software will wait for a TCP session to reach the established state before dropping the session.
ip inspect udp idle-time	Specifies the UDP idle timeout (the length of time for which a UDP session will still be managed while there is no activity).

ip inspect tcp finwait-time

To define how long a TCP session will still be managed after the firewall detects a FIN-exchange, use the **ip inspect tcp finwait-time** command in global configuration mode. To reset the timeout to the default of 5 seconds, use the **no** form of this command.

ip inspect tcp finwait-time *seconds* [**vrf** *vrf-name*]

no ip inspect tcp finwait-time

Syntax Description

seconds	Specifies how long a TCP session will be managed after the firewall detects a FIN-exchange. The default is 5 seconds.
vrf *vrf-name*	(Optional) Defines the information only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

5 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the software detects a valid TCP packet that is the first in a session, and if Context-based Access Control (CBAC) inspection is configured for the protocol of the packet, the software establishes state information for the new session.

Use this command to define how long TCP session state information will be maintained after the firewall detects a FIN-exchange for the session. The FIN-exchange occurs when the TCP session is ready to close.

The global value specified for this timeout applies to all TCP sessions inspected by CBAC.

The timeout set with this command is referred to as the “finwait” timeout.

Note If the -n option is used with rsh, and the commands being executed do not produce output before the “finwait” timeout, the session will be dropped and no further output will be seen.

Examples

The following example changes the finwait timeout to 10 seconds:

```
ip inspect tcp finwait-time 10
```

The following example changes the finwait timeout back to the default (5 seconds):

```
no ip inspect tcp finwait-time
```

ip inspect tcp idle-time

To specify the TCP idle timeout (the length of time a TCP session will still be managed while there is no activity), use the **ip inspect tcp idle-time** command in global configuration mode. To reset the timeout to the default of 3600 seconds (1 hour), use the **no** form of this command.

ip inspect tcp idle-time *seconds* [**vrf** *vrf-name*]

no ip inspect tcp idle-time

Syntax Description

seconds	Specifies the length of time, in seconds, for which a TCP session will still be managed while there is no activity. The default is 3600 seconds (1 hour).
vrf *vrf-name*	(Optional) Specifies the TCP idle timer only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

3600 seconds (1 hour)

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the software detects a valid TCP packet that is the first in a session, and if Context-based Access Control (CBAC) inspection is configured for the packet's protocol, the software establishes state information for the new session.

If the software detects no packets for the session for a time period defined by the TCP idle timeout, the software will not continue to manage state information for the session.

The global value specified for this timeout applies to all TCP sessions inspected by CBAC. This global value can be overridden for specific interfaces when you define a set of inspection rules with the **ip inspect name** (global configuration) command.

Note This command does not affect any of the currently defined inspection rules that have explicitly defined timeouts. Sessions created based on these rules still inherit the explicitly defined timeout value. If you change the TCP idle timeout with this command, the new timeout will apply to any new inspection rules you define or to any existing inspection rules that do not have an explicitly defined timeout. That is, new sessions based on these rules (having no explicitly defined timeout) will inherit the global timeout value.

Examples

The following example sets the global TCP idle timeout to 1800 seconds (30 minutes):

```
ip inspect tcp idle-time 1800
```

The following example sets the global TCP idle timeout back to the default of 3600 seconds (one hour):

```
no ip inspect tcp idle-time
```

ip inspect tcp max-incomplete host

To specify threshold and blocking time values for TCP host-specific denial-of-service (DoS) detection and prevention, use the **ip inspect tcp max-incomplete host** command in global configuration mode. To reset the threshold and blocking time to the default values, use the **no** form of this command.

ip inspect tcp max-incomplete host *number* **block-time** *minutes* [**vrf** *vrf-name*]

no ip inspect tcp max-incomplete host

Syntax Description

number	Specifies how many half-open TCP sessions with the same host destination address can exist at a time, before the software starts deleting half-open sessions to the host. Use a number from 1 to 250. The default is 50 half-open sessions.
block-time	Specifies blocking of connection initiation to a host.
minutes	Specifies how long the software will continue to delete new connection requests to the host. The default is 0 minutes.
vrf *vrf-name*	(Optional) Specifies the information only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

50 half-open sessions and 0 minutes

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

An unusually high number of half-open sessions with the same destination host address could indicate that a denial-of-service attack is being launched against the host. For TCP, “half-open” means that the session has not reached the established state.

Whenever the number of half-open sessions with the same destination host address rises above a threshold (the **max-incomplete host** number), the software will delete half-open sessions according to one of the following methods:

- If the **block-time** *minutes* timeout is 0 (the default):

  The software will delete the oldest existing half-open session for the host for every new connection request to the host. This ensures that the number of half-open sessions to a given host will never exceed the threshold.

- If the **block-time** *minutes* timeout is greater than 0:

  The software will delete all existing half-open sessions for the host, and then block all new connection requests to the host. The software will continue to block all new connection requests until the **block-time** expires.

The software also sends syslog messages whenever the **max-incomplete host** number is exceeded and when blocking of connection initiations to a host starts or ends.

The global values specified for the threshold and blocking time apply to all TCP connections inspected by Context-based Access Control (CBAC).

Examples

The following example changes the max-incomplete host number to 40 half-open sessions, and changes the block-time timeout to 2 minutes:

```
ip inspect tcp max-incomplete host 40 block-time 2
```

The following example resets the defaults (50 half-open sessions and 0 minutes):

```
no ip inspect tcp max-incomplete host
```

Related Commands

Command	Description
ip inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ip inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ip inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ip inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.

ip inspect tcp reassembly

To set parameters that define how Cisco IOS Firewall application inspection and Cisco IOS Intrusion Prevention System (IPS) will handle out-of-order TCP packets, use the **ip inspect tcp reassembly** command in global configuration mode. To disable at least one defined parameter, use the **no** form of this command.

ip inspect tcp reassembly {**alarm** {**on** | **off**} | **memory limit** *size-in-kb* | **queue length** *number-of-packets* | **timeout** *seconds*} [**vrf** *vrf-name*]

no ip inspect tcp reassembly {**alarm** | **queue length** | **timeout** | **memory limit**} [**vrf** *vrf-name*]

Syntax Description

alarm {**on** | **off**}	Specifies the alert message configuration. If enabled, a syslog message is generated when an out-of-order packet is dropped. Default value: **on**
memory	Specifies the memory use allowed by the TCP reassembly module.
limit *size-in-kb*	Specifies the limit of out of order queue size.
queue	Specifies the out of order queue parameters.
length *number-of-packets*	Maximum number of out-of-order packets that can be held per queue (buffer). (There are two queues per session.) Available value range: 0 to 1024. Default value: 16. **Note** If the queue length is set to 0, all out-of-order packets are dropped; that is, TCP out-of-order packet buffering and reassembly is disabled.
timeout *seconds*	Number of seconds the TCP reassembly module will hold out-of-order segments that are waiting for the first segment missing in the sequence. After the timeout timer has expired, a retry timer is started. The value for the retry timer is four times the configured timeout value.
vrf *vrf-name*	Specifies the VPN routing and forwarding (VRF) parameter and name.

Command Default

Queue length: 16

Memory Limit: 1024 kilobytes

Alarm: on

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(11)T	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

The queue length Value

The value specified for the queue length is applicable for two queues per session: one queue is for the initiator traffic and the other queue is for the responder traffic. For example, the default queue size is 16. Thus, up to 16 packets can be held per queue, so 16 packets per queue results in a maximum of 32 packets per session.

When the maximum queue length value is reached, the packet being switched is dropped unless it is the packet that will be processed by a firewall or IPS. If the packet is dropped, a syslog message, which explains why the packet was dropped, will be generated. (To generate syslog messages, you must have the alarm option set to "on.")

The timeout Value

When a timer expires for the first time, the packets in the queue are not deleted. However, after the retry timer expires, the session is deleted, a syslog message is generated, and all unprocessed, out-of-order packets still in the queue are deleted.

The memory limit Value

When the limit for TCP reassembly memory is reached, packets from the reassembly queue of the current session are released so incoming packets can be accepted. Packets from the end of the queue are released to ensure that they are farthest away from the hole that is to be filled. However, if the queue is empty and the maximum memory has been reached, the incoming packet is dropped.

The alarm Value

If an alarm value is not configured, the value is set to "on," unless the **ip inspect alarm** command is enabled and set to off; thus, syslog messages related to TCP connections will not be generated. However, if the alarm value for this command is set to "on" and the **ip inspect alarm** command is set to "off," the value of the **ip inspect alarm** command is ignored and syslog messages are generated.

The alarm value is independent of and in addition to the syslog messages that can be enabled for a Cisco IOS Firewall or Cisco IOS IPS.

Examples

The following example shows how to instruct Cisco IOS IPS how to handle out-of-order packets for TCP connections:

```
Router(config)# ip inspect tcp reassembly queue length 18
Router(config)# ip inspect tcp reassembly memory limit 200
```

Related Commands

Command	Description
ip inspect tcp block-non-session	Blocks packets that do not belong to the existing firewall TCP sessions in the inbound and outbound directions.

ip inspect tcp synwait-time

To define how long the software will wait for a TCP session to reach the established state before dropping the session, use the **ip inspect tcp synwait-time** command in global configuration mode. To reset the timeout to the default of 30 seconds, use the **no** form of this command.

ip inspect tcp synwait-time *seconds* [**vrf** *vrf-name*]

no ip inspect tcp synwait-time

Syntax Description

seconds	Specifies how long, in seconds, the software will wait for a TCP session to reach the established state before dropping the session. The default is 30 seconds.
vrf *vrf-name*	(Optional) Defines the information only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

30 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to define how long Cisco IOS software will wait for a TCP session to reach the established state before dropping the session. The session is considered to have reached the established state after the first synchronize sequence number (SYN) bit of the session is detected.

The global value specified for this timeout applies to all TCP sessions inspected by Context-based Access Control (CBAC).

Examples

The following example changes the synwait timeout to 20 seconds:

```
ip inspect tcp synwait-time 20
```

The following example changes the synwait timeout back to the default (30 seconds):

```
no ip inspect tcp synwait-time
```

ip inspect tcp window-scale-enforcement loose

To configure Cisco IOS software to disable the window scale option check for a TCP packet that has an invalid window scale option under the Context-Based Access Control (CBAC) firewall, use the **ip inspect tcp window-scale-enforcement loose** command in global configuration mode. To return to the command default, use the **no** form of this command.

ip inspect tcp window-scale-enforcement loose

no ip inspect tcp window-scale-enforcement loose

Command Default

The strict window scale option check is enabled in the firewall by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The window scale extension expands the definition of the TCP window to 32 bits and then uses a scale factor to carry this 32-bit value in the 16-bit Window field of the TCP header. Cisco IOS software enforces strict checking of the TCP window scale option. See section 2 of RFC1323, "TCP Window Scale Option," for more information on this function.

There are occasions when a server may be using a non-RFC compliant TCP/IP protocol stack. In this case, the initiator does not offer the window scale option, but the responder has the option enabled with a window scale factor that is not zero.

Cisco IOS administrators who experience issues with a noncompliant server may not have control over the client to which they need to connect. Disabling the Cisco IOS firewall to connect to the noncompliant server is not desirable and may fail if each endpoint cannot agree on the window scaling factor to use for its respective receive window.

The **ip inspect tcp window-scale-enforcement loose** command is used in global configuration mode to allow noncompliant window scale negotiation and works without the firewall being disabled to access the noncompliant servers. This command works under the CBAC firewall, which intelligently filters TCP and UDP packets based on application-layer protocol session information. CBAC inspects traffic that travels through the firewall to discover and manage state information for TCP and UDP sessions. CBAC is configured using an inspect rule only on interfaces. This state information is used to create temporary openings in the firewall's access lists to allow return traffic and additional data connections for permissible sessions. Traffic entering or leaving the configured interface is inspected based on the direction that the inspect rule was applied.

Examples

The following example configures the IOS to disable the window scale option check in the CBAC firewall for a TCP packet that has an invalid window scale option:

```
Router# config
Router(config)# ip inspect tcp window-scale-enforcement loose
```

Related Commands

Command	Description
ip inspect tcp synwait-time	Configures the length of time the software waits for a TCP session to reach the established state before dropping the session.

ip inspect udp idle-time

To specify the User Datagram Protocol (UDP) idle timeout (the length of time for which a UDP "session" will still be managed while there is no activity), use the **ip inspect udp idle-time** command in global configuration mode. To reset the timeout to the default of 30 seconds, use the **no** form of this command.

ip inspect udp idle-time *seconds* [**vrf** *vrf-name*]

no ip inspect udp idle-time

Syntax Description

seconds	Specifies the length of time a UDP "session" will still be managed while there is no activity. The default is 30 seconds.
vrf *vrf-name*	(Optional) Specifies the UDP idle timeout only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

30 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the software detects a valid UDP packet, if Context-based Access Control (CBAC) inspection is configured for the packet's protocol, the software establishes state information for a new UDP "session." Because UDP is a connectionless service, there are no actual sessions, so the software approximates sessions by examining the information in the packet and determining if the packet is similar to other UDP packets (for example, it has similar source or destination addresses) and if the packet was detected soon after another similar UDP packet.

If the software detects no UDP packets for the UDP session for the a period of time defined by the UDP idle timeout, the software will not continue to manage state information for the session.

The global value specified for this timeout applies to all UDP sessions inspected by CBAC. This global value can be overridden for specific interfaces when you define a set of inspection rules with the **ip inspect name** command.

Note This command does not affect any of the currently defined inspection rules that have explicitly defined timeouts. Sessions created based on these rules still inherit the explicitly defined timeout value. If you change the UDP idle timeout with this command, the new timeout will apply to any new inspection rules you define or to any existing inspection rules that do not have an explicitly defined timeout. That is, new sessions based on these rules (having no explicitly defined timeout) will inherit the global timeout value.

Examples

The following example sets the global UDP idle timeout to 120 seconds (2 minutes):

```
ip inspect udp idle-time 120
```

The following example sets the global UDP idle timeout back to the default of 30 seconds:

```
no ip inspect udp idle-time
```

integrity

To specify one or more integrity algorithms for an Internet Key Exchange Version 2 (IKEv2) proposal, use the **integrity** command in IKEv2 proposal configuration mode. To remove the configuration of the hash algorithm, use the **no** form of this command.

integrity {**sha1** | **sha256** | **sha384** | **md5**}

no integrity

Syntax Description

sha1	Specifies Secure Hash Algorithm (SHA-1 - HMAC variant) as the hash algorithm.
sha256	Specifies SHA-2 family 256-bit (HMAC variant) as the hash algorithm.
sha384	Specifies SHA-2 family 384-bit (HMAC variant) as the hash algorithm.
md5	Specifies Message-Digest algorithm 5 (MD5 - HMAC variant) as the hash algorithm.

Command Default

The default integrity algorithm is used.

Command Modes

IKEv2 proposal configuration (config-ikev2-proposal)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(2)T	This command was modified. The **sha256** and **sha384** keywords were added.

Usage Guidelines

Use this command to specify the integrity algorithm to be used in an IKEv2 proposal. The default integrity algorithms in the default proposal are SHA-1 and MD5.

Note You cannot selectively remove an integrity algorithm when multiple integrity algorithms are configured.

Suite-B adds support for the SHA-2 family (HMAC variant) hash algorithm used to authenticate packet data and verify the integrity verification mechanisms for the IKEv2 proposal configuration. HMAC is a variant that provides an additional level of hashing.

Examples

The following example configures an IKEv2 proposal with the MD5 integrity algorithm:

```
Router(config)# crypto ikev2 proposal proposal1
Router(config-ikev2-proposal)# integrity md5
```

Related Commands

Command	Description
crypto ikev2 proposal	Defines an IKEv2 proposal.
encryption (ikev2 proposal)	Specifies the encryption algorithm in an IKEv2 proposal.
group (ikev2 proposal)	Specifies the Diffie-Hellman group identifier in an IKEv2 proposal.
show crypto ikev2 proposal	Displays the parameters for each IKEv2 proposal.

ip interface

To configure a virtual gateway IP interface on a Secure Socket Layer Virtual Private Network (SSL VPN) gateway, use the **ip interface** command in webvpn gateway configuration mode. To disable the configuration, use the **no** form of this command.

ip interface *type number* [**port** {**443** | *port-number*}]

no ip interface

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
port	(Optional) Configures a specific port on the gateway.
443	(Optional) Configures the default secure port.
port-number	(Optional) Port number to be configured on the SSL VPN gateway. Range: 1025 to 65535. Default: 443.

Command Default

The command is disabled. The virtual gateway IP address is not configured.

Command Modes

Webvpn gateway configuration (config-webvpn-gateway)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **ip interface** command is used to configure a interface on a SSL VPN gateway. You can use this command to configure the WebVPN gateway to retrieve the IP address from an interface, and if you do not want to configure the IP address manually. This command is useful when the public interface is Dynamic Host Configuration Protocol (DHCP) and you do not know the IP address or when the IP address gets changed.

If the **ip interface** command is not configured then the WebVPN will use the IP address configured using the **ip address** command.

Examples

The following example shows how to configure a virtual gateway IP interface on port 1036 of an SSL VPN gateway:

```
Router# configure terminal
Router(config)# webvpn gateway gateway1
Router(config-webvpn-gateway)# ip interface FastEthernet 0/1 port 1036
```

Related Commands

Command	Description
ip address	Configures a proxy IP address on an SSL VPN gateway.
webvpn gateway	Defines an SSL VPN gateway and enters WebVPN gateway configuration mode.

ip ips

To apply an Intrusion Prevention System (IPS) rule to an interface, use the **ip ips** command in interface configuration mode. To remove an IPS rule from an interface direction, use the **no** form of this command.

ip ips *ips-name* {**in** | **out**}

no ip ips *ips-name* {**in** | **out**}

Syntax Description

ips-name	Name of IPS signature definition file (SDF).
in	Applies IPS to inbound traffic.
out	Applies IPS to outbound traffic.

Defaults

By default, IPS signatures are not applied to an interface or direction.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	The command name was changed from the **ip audit** command to the **ip ips** command.

Usage Guidelines

The **ip ips** command loads the SDF onto the router and builds the signature engines when IPS is applied to the first interface.

Note The router prompt disappears while the signatures are loading and the signature engines are building. It will reappear after these tasks are complete.

Depending on your platform and how many signatures are being loaded, building the signature engine can take several of minutes. It is recommended that you enable logging messages so you can monitor the engine building status.

The **ip ips** command replaces the **ip audit** command. If the **ip audit** command is part of an existing configuration, IPS will interpret it as the **ip ips** command.

Examples

The following example shows the basic configuration necessary to load the attack-drop.sdf file onto a router running Cisco IOS IPS. Note that the configuration is almost the same as when you load the default signatures onto a router, except for the **ip ips sdf location** command, which specifies the attack-drop.sdf file.

```
!
ip ips sdf location disk2:attack-drop.sdf
```

```
ip ips name MYIPS
!
interface GigabitEthernet0/1
 ip address 10.1.1.16 255.255.255.0
 ip ips MYIPS in
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
!
```

The following example shows how to configure the router to load and merge the attack-drop.sdf file with the default signatures. After you have merged the two files, it is recommended to copy the newly merged signatures to a separate file. The router can then be reloaded (via the **reload** command) or reinitalized to so as to recognize the newly merged file (as shown the following example)

```
!
ip ips name MYIPS
!
interface GigabitEthernet0/1
 ip address 10.1.1.16 255.255.255.0
 ip ips MYIPS in
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
!
!
! Merge the flash-based SDF (attack-drop.sdf) with the built-in signatures.
copy disk2:attack-drop.sdf ips-sdf
! Save the newly merged signatures to a separate file.
copy ips-sdf disk2:my-signatures.sdf
!
! Configure the router to use the new file, my-signatures.sdf
configure terminal
ip ips sdf location disk2:my-signatures.sdf
! Reinitialize the IPS by removing the IPS rule set and reapplying the rule set.
interface gig 0/1
 no ip ips MYIPS in
!
*Apr 8 14:05:38.243:%IPS-2-DISABLED:IPS removed from all interfaces - IPS disabled
!
 ip ips MYIPS in
!
 exit
```

Related Commands

Command	Description
copy ips-sdf	Loads or saves the SDF in the router.
ip ips sdf location	Specifies the location in which the router should load the SDF.

ip ips auto-update

To enable automatic signature updates for Cisco IOS Intrusion Prevention System (IPS), use the **ip ips auto-update** command in global configuration mode. To revert back to the default value, use the **no** form of this command.

ip ips auto-update

no ip ips auto-update

Syntax Description

This command has no arguments or keywords.

Command Default

The default value is defined in the signature definition XML.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Automatic signature updates allow users to override the existing IPS configuration and automatically keep signatures up to date on the basis of a preset time, which can be configured to a preferred setting.

Use the **ip ips auto-update** command to enable Cisco IOS IPS to automatically update the signature file on the system. When enabling automatic signature updates, it is recommended that you ensure the following configuration guidelines have been met:

- The router's clock is set up with the proper relative time.
- The frequency for Cisco IOS IPS to obtain updated signature information has been defined (through the **occur-at** command).
- Automatic signature updates can be enabled from Cisco.com by using the **cisco** command. This command cannot be used in conjunction with the **url** command.
- The URL in which to retrieve the Cisco IOS IPS signature configuration files has been specified (through the **url** command).
- Optionally, the username and password in which to access the files from the server has been specified (through the **username** command). The **username** command would be optional in this case if the username and password command were previously configured through the **ips signature update cisco** command in Priviledged EXEC mode. The user name and password must be configured for updating signatures directly from Cisco.com.

The Default Value

A user or a management station can override the default value through the **category** command or the **signature** command; a value set with either of these commands will be saved as the delta value. The no form of the ip ips auto-update command will remove the delta value and revert back to the default value in the definition XML.

Setting Time for Auto Updates

Cisco IOS time can be updated through the hardware clock or the software configurable clock (which ever option is available on your system). Although Network Time Protocol (NTP) is typically used for automated time synchronization, Cisco IOS IPS updates use the local clock resources as a reference for update intervals. Thus, NTP should be configured to update the local time server of the router, as appropriate.

Examples

The following example shows how to configure automatic signature updates and issue the **show ip ips auto-update** command to verify the configuration. In this example, the signature package file is pulled from the TFTP server at the third hour of the 5 day of the month, at the 56th minute of this hour. (Note that adjustments are made for months without 31 days and daylight savings time.)

```
Router# clock set ?
    hh:mm:ss Current Time
Router# clock set 10:38:00 20 apr 2006
Router#
*Apr 20 17:38:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 10:37:55 MST
Thu Apr 20 2006 to 10:38:00 MST Thu Apr 20 2006, configured from console by cisco on
console.

Router(config)# ip ips auto-update
Router(config-ips-auto-update)# occur-at monthly 5 56 3
Router#
*May 4 2006 15:50:28 MST: IPS Auto Update: setting update timer for next update: 5 days 56
min 3 hrs
*May 4 2006 15:50:28 MST: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router#
Router# show ip ips auto-update

IPS Auto Update Configuration
    URL : tftp://192.168.0.2/jdoe/ips-auto-update/IOS_reqSeq-dw.xml
    Username : not configured
    Password : not configured
    Auto Update Intervals
      minutes (0-59) : 56
      hours (0-23) : 3
      days of month (1-31) : 5
      days of week: (0-6) :
```

Related Commands

Command	Description
occur-at	Defines the frequency in which Cisco IOS IPS obtains updated signature information.
cisco	Enables automatic signature updates from Cisco.com.
url (ips-autoupdate)	Defines a location in which to retrieve the Cisco IOS IPS signature configuration files.
username (ips-autoupdate)	Defines a username and password in which to access signature files from the server.

ip ips config location

To specify the location in which the router will save signature information, use the **ip ips config location** command in global configuration mode. To remove the specified location, use the **no** form of this command.

ip ips config location *url*

no ip ips config location

Syntax Description

url	Location where the signature file is saved. Available URL options: • Local flash, such as flash:sig.xml • FTP server, such as ftp://myuser:mypass@ftp_server.sig.xml • rcp, such as rcp://myuser@rcp_server/sig.xml • TFTP server, such as tftp://tftp_server/sig.xml **Note** If the specified location is a URL, such as an FTP server, the user must have writer privileges.

Command Default

No configuration files are saved.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Before configuring the **ip ips config location** command, you must create a directory for the config location via the **mkdir** command.

The **ip ips config location** command configures a Cisco IOS Intrusion Prevention System (IPS) signature location, which tells Cisco IOS IPS where to save signature information.

The configuration location is used to restore the IPS configuration in cases such as router reboots or IPS becoming disabled or reenabled. Files, such as signature definitions, signature-type definitions, and signature category information, are written in XML format, compressed, and saved to the specified IPS signature location.

Note If a location is not specified, or if a location is removed via the **no** form, no files will be saved.

Note The **ip ips config location** command replaces the **ip ips sdf location** command.

Examples

The following example shows how to instruct the router to save all signature information to the directory "flash:/ips5":

```
Router# mkdir flash:/ips5
Create directory filename [ips5]?
Created dir flash:/ips5
Router#
Router#
Router#
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ips name MYIPS
Router(config)# ip ips config location flash:/ips5
Router(config)# ip ips signature-category
Router(config-ips-category)# category all
Router(config-ips-category-action)# retired true
Router(config-ips-category-action)# exit
Router(config-ips-category)# category ios_ips advanced
Router(config-ips-category-action)# retired false
Router(config-ips-category-action)# exit
Router(config-ips-category)# exit
Do you want to accept these changes? [confirm]
Router(config)# d
*Nov 14 2006 17:16:42 MST: Applying Category configuration to signatures ..
Router(config)#
```

ip ips deny-action ips-interface

To create an access control list (ACL) filter for the deny actions ("denyFlowInline" and "denyConnectionInline") on the intrusion prevention system (IPS) interface rather than ingress interface, use the **ip ips deny-action ips-interface** command in global configuration mode. To return to the default, use the **no** form of this command.

ip ips deny-action ips-interface

no ip ips deny-action ips-interface

Syntax Description

This command has no arguments or keywords.

Defaults

ACLs filter for the deny actions are applied to the ingress interface.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use the **ip ips deny-action ips-interface** command to change the default behavior of the ACL filters that are created for the deny actions.

Note You should configure this command only if at least one signature is configured to use the supported deny actions (denyFlowInline and denyConnectionInline, if the input interface is configured to for load balancing, and if IPS is configured on the output interface.

Default ACL Filter Approach

By default, ACL filters for the deny actions are created on the ingress interfaces of the offending packet. Thus, if Cisco IOS IPS is configured in outbound direction on the egress interface and the "deny" ACLs are created on the ingress interface, Cisco IOS IPS will drop the matching traffic before it goes through much processing. Unfortunately, this approach does not work in load balancing scenarios for which there is more than one ingress interface performing load-balancing.

Alternative ACL Filter Approach

The **ip ips deny-action ips-interface** command enables ACLs to be created on the same interface and in the same direction as Cisco IOS IPS is configured. This alternative approach supports load-balancing scenarios—assuming that the load-balancing interfaces have the same Cisco IOS IPS configuration. However, all outbound Cisco IOS IPS traffic will go through substantial packet path processing before it is eventually dropped by the ACLs.

Examples

The following example shows how to configure load-balancing between interface e0 and interface e1:

```
ip ips name test
ip ips deny-action ips-interface
! Enables load balancing with e1
interface e0
 ip address 10.1.1.14 255.255.255.0
 no shut
!
! Enables load balancing with e0
interface e1
 ip address 10.1.1.16 255.255.255.0
 no shut
!
interface e2
 ip address 10.1.1.18 255.255.255.0
 ip ips test in
 no shut
```

ip ips enable-clidelta

To enable the signature tuning settings in the clidelta.xmz file on the router to take precedence over the signature settings in the intrusion prevention system (IPS) iosips-sig-delta.xmz file, use the **ip ips enable-clidelta** command in global configuration mode. To restore precedence to the iosips-sig-delta.xmz file settings, use the no form of this command.

ip ips enable-clidelta

no ip ips enable-clidelta

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

Most IPS devices and applications provide either a single default configuration or multiple default configurations. Using one of these default configurations is an ideal starting point for deploying IPS. When IOS IPS is deployed, parameters such as severity, active status, or event actions of certain signatures need to be tuned to meet the requirements of an enterprise network traffic profile.

Once the **ip ips enable-clidelta** command is enabled, a local cli-delta.xmz file is generated containing the local tuning signatures configured through the CLI. The settings in the clidelta.xmz file take precedence when a globally administered delta signature update, contained in the iosips-sig-delta.xmz file, is sent from a central repository and applied to the configuration of the local router.

Examples

The following example shows how to enable the clidelta functionality:

```
Router(config)# ip ips enable-clidelta
```

Related Commands

Command	Description
show ip ips sig-clidelta	Displays information about the IPS iosips-sig-clidelta.xmz file on the router to verify signature tuning settings.

ip ips event-action-rules

To enter config-rule configuration mode, which allows users to change the target value rating, use the **ip ips event-action-rules** command in global configuration mode.

ip ips event-action-rules

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

You must issue the **ip ips event-action-rules** command to define the target value rating via the **target-value** command.

Examples

The following example shows how to change the target value to low for the host 192.168.0.1:

```
configure terminal
ip ips event-action-rules
 target-value low target-address 192.168.0.1
```

Related Commands

Command	Description
target-value	Defines the target value rating for a host.

ip ips fail closed

To instruct the router to drop all packets until the signature engine is built and ready to scan traffic, use the **ip ips fail closed** command in global configuration mode. To return to the default functionality, use the **no** form of this command.

ip ips fail closed

no ip ips fail closed

Syntax Description

This command has no arguments or keywords.

Defaults

All packets are passed without being scanned while the signature engine is being built or if the signature engine fails to build.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Cisco IOS IPS Fails to Load the SDF

By default, the router running Intrusion Prevention System (IPS) will load the built-in signatures if it fails to load the signature definition file (SDF). If this command is issued, the router will drop all packets—unless the user specifies an access control list (ACL) for packets to send to IPS.

IPS Loads the SDF but Fails to Build a Signature Engine

If the router running IPS loads the SDF but fails to build a signature engine, the router will mark the engine "not ready." If an available engine is previously loaded, the IPS will keep the available engine and discard the engine that is not ready for use. If no previous engines have been loaded or "not ready," the router will install the engine that is not ready and rely on the configuration of the **ip ips fail closed** command.

By default, packets destined for an engine marked "not ready" will be passed without being scanned. If this command is issued, the router will drop all packets that are destined for that signature engine.

Examples

The following example shows how to instruct the router to drop all packets if the SME is not yet available:

```
Router(config)# ip ips fail closed
```

ip ips inherit-obsolete-tunings

To enable Cisco IOS Intrusion Prevention System (IPS) signatures to inherit tunings from obsoleted signatures in a Cisco IOS IPS, use the **ip ips inherit-obsolete-tunings** command in global configuration mode. To disable this function, use the **no** form of this command.

ip ips inherit-obsolete-tunings

no ip ips inherit-obsolete-tunings

SyntaxDescription This command has no arguments or keywords.

Command Default Tunings from obsoleted signatures in Cisco IOS IPS are not inherited.

Command Modes Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines The **ip ips inherit-obsolete-tunings** command enables new signatures to obsolete older signatures and inherit the event-action and enabled parameters of the obsolete tuning values without the need to manually tune the new signatures. All other parameter changes, including the “Retire” parameter saved in the old signatures, will be ignored.

After you enter the command, the screen displays a warning message asking you to clarify the intended usage and then asks whether you accept the configuration, By default, old signatures tunings are not inherited by new signatures.

Note The tunings of old signatures will be lost if they are not migrated to new signatures.

Note To enable inheritance of tunings, configure the **ip ips inherit-obsolete-tunings** command before a signature file is loaded.

Note Users of management devices should use those devices and not enable the **ip ips inherit-obsolete-tunings** command.

Examples

The following example shows how to configure a router running Cisco IOS IPS to allow new signatures to inherit the tuning values from the obsoleted signatures, without having to manually tune the new signatures:

```
Router(config)# ip ips inherit-obsolete-tunings
```

Related Commands

Command	Description
ip ips	Applies a IPS rule to an interface.
ip ips memory regex chaining	Enables an Cisco IOS IPS to chain multiple regex tables together and load additional signatures.
ip ips memory threshold	Specifies an Cisco IOS IPS memory threshold.
show ip ips	Displays Cisco IOS IPS information such as configured sessions and signatures.

ip ips memory regex chaining

To enable a Cisco IOS Intrusion Prevention System (IPS) to chain multiple regex tables together and load additional signatures, use the **ip ips memory regex chaining** command in global configuration mode. To disable this function, use the **no** form of this command.

ip ips memory regex chaining

no ip ips memory regex chaining

Syntax Description

This command has no arguments or keywords.

Command Default

Multiple regex table chaining is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Multiple regex table chaining is used to load additional signatures when a Cisco IOS IPS is supporting a large signature set. The default is three chained tables when the **ip ips memory regex chaining** command is enabled. This results in slower performance of Cisco IOS IPS scanning due to scanning packets across more than a single regex table.

When a user tries to load a specific set of signatures that does not fit using a single table, compilation errors will result. A compiler failure error message looks like this:

```
*Sep  9 17:27:46.907: %IPS-4-SIGNATURE_COMPILE_FAILURE: string-tcp 3730:0 - compiles
discontinued for this engine
```

Examples

The following example shows how to enable the **ip ips memory regex chaining** command:

```
Router(config)# ip ips memory regex chaining
```

Related Commands

Command	Description
ip ips	Applies an IPS rule to an interface.
ip ips inherit-obsolete-tunings	Applies tunings from obsoleted signatures to the new versions of the signatures.
ip ips memory threshold	Specifies a Cisco IOS IPS memory threshold.
show ip ips	Displays Cisco IOS IPS information such as configured sessions and signatures.

ip ips memory threshold

To specify a memory threshold when using a Cisco IOS Intrusion Prevention System (IPS), use the **ip ips memory threshold** command in global configuration mode. To disable this function, use the **no** form of this command.

ip ips memory threshold *megabytes*

no ip ips memory threshold

Syntax Description

megabytes	The IPS memory threshold, in megabytes. The valid range is from 0-1024.

Command Default

The default IPS memory threshold is 10 percent of free memory—this is available for router operations other than Cisco IOS IPS.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

The IPS memory threshold defines the amount of free memory unavailable to the IPS.

When you are loading signatures, the default state is that Cisco IOS IPS cannot consume any more memory if the remaining (free) memory becomes less than 10 percent of the size of the total DRAM installed on the router (for example, less than 25.6 MB free memory left on routers with 256 MB DRAM). The 10 percent of free memory unavailable to IPS defines the IPS memory threshold. The IPS memory threshold can be changed using the **ip ips memory threshold** command to force IPS to use less memory, so that other features get access to more memory if they need it.

Setting a memory threshold for Cisco IOS IPS is recommended especially when an arbitrary number of signatures may be added on top of the recommended sets in Cisco IOS IPS Basic or Advanced/Default categories, or when a fully customized signature set is created and loaded.

Examples

The following example shows how to configure a router running Cisco IOS IPS to set the IPS memory threshold to a value of 50 MB:

```
Router(config)# ip ips memory threshold 50
```

Related Commands

Command	Description
ip ips	Applies an IPS rule to an interface.
ip ips inherit-obsolete-tunings	Applies tunings from obsoleted signatures to the newer versions of the signatures.

Command	Description
ip ips memory regex chaining	Enables a Cisco IOS IPS to chain multiple regex tables together and load additional signatures.
show ip ips	Displays Cisco IOS IPS information such as configured sessions and signatures.

ip ips name

To specify an intrusion prevention system (IPS) rule, use the **ip ips name** command in global configuration mode. To delete an IPS rule, use the **no** form of this command.

ip ips name *ips-name* [**list** *acl*]

no ip ips name *ips-name* [**list** *acl*]

Syntax Description

ips-name	Name for IPS rule.
list *acl*	(Optional) Specifies an extended or standard access control list (ACL) to filter the traffic that will be scanned. **Note** All traffic that is permitted by the ACL is subject to inspection by the IPS. Traffic that is denied by the ACL is not inspected by the IPS.

Defaults

An IPS rule does not exist.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	The command name was changed from the **ip audit name** command to the **ip ips name** command.

Usage Guidelines

The IPS does not load the signatures until the rule is applied to an interface via the **ip ips** command.

Note This command replaces the **ip audit name** global configuration command. If the **ip audit name** command has been issued in an existing configuration and an access control list (ACL) has been defined, IPS will apply the **ip ips name** command and the ACL parameter on all interfaces that applied the rule.

Examples

The following example shows how to configure a router running Cisco IOS IPS to load the default, built-in signatures. Note that a configuration option for specifying an SDF location is not necessary; built-in signatures reside statically in Cisco IOS.

```
!
ip ips po max-events 100
ip ips name MYIPS
!
interface GigabitEthernet0/1
 ip address 10.1.1.16 255.255.255.0
 ip ips MYIPS in
 duplex full
 speed 100
```

```
 media-type rj45
 no negotiation auto
!
```

Related Commands

Command	Description
ip ips	Applies an IPS rule to an interface.
show ip ips	Displays IPS information such as configured sessions and signatures.

ip ips notify

To specify the method of event notification, use the **ip ips notify** command in global configuration mode. To disable event notification, use the **no** form of this command.

ip ips notify [**log** | **sdee**]

no ip ips notify [**log** | **sdee**]

Syntax Description

log	(Optional) Send messages in syslog format. **Note** If an option is not specified, alert messages are sent in syslog format.
sdee	(Optional) Send messages in Security Device Event Exchange (SDEE) format.

Defaults

By default, event notification through syslog is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	The command name was changed from the **ip audit notify** command to the **ip ips notify** command. Also, support for SDEE was introduced, and the **sdee** keyword was added.
12.3(14)T	The Post Office protocol was deprecated, and the **nr-director** keyword was removed.

Usage Guidelines

SDEE is always running, but it does not receive and process events from Intrusion Prevention System (IPS) unless SDEE notification is enabled. If it is not enabled and a client sends a request, SDEE will respond with a fault response message, indicating that notification is not enabled.

To use SDEE, the HTTP server must be enabled (via the **ip http server** command). If the HTTP server is not enabled, the router cannot respond to the SDEE clients because it cannot not see the requests.

Note The **ip ips notify** command replaces the **ip audit notify** command. If the **ip audit notify** command is part of an existing configuration, the IPS will interpret it as the **ip ips notify** command.

Examples

In the following example, event notifications are specified to be sent in SDEE format:

```
ip ips notify sdee
```

Related Commands

Command	Description
ip http server	Enables the HTTP server on your system.

ip ips sdf location

Note In Cisco IOS Release 12.4(11)T, the **ip ips sdf location** command was replaced with the **ip ips config location** command. For more information, see the **ip ips config location** command.

To specify the location in which the router will load the signature definition file (SDF), use the **ip ips sdf location** command in global configuration mode. To remove an SDF location from the configuration, use the **no** form of this command.

ip ips sdf location *url* [**retries** *number* **wait-time** *seconds*] [**autosave**]

no ip ips sdf location *url* [**retries** *number* **wait-time** *seconds*] [**autosave**]

Syntax Description

url	Location of the SDF. Available URL options: • local flash, such as flash:sig.xml • FTP server, such as ftp://myuser:mypass@ftp_server.sig.xml • rcp, such as rcp://myuser@rcp_server/sig.xml • TFTP server, such as tftp://tftp_server/sig.xml
retries *number*	(Optional) Number of times the router will try to load the SDF after the first attempt fails.
wait-time *seconds*	(Optional) Duration, in seconds, between retry attempts.
autosave	(Optional) Specifies that the router will save a new SDF to the specified location.

Defaults

If an SDF location is not specified, the router will load the default built-in signatures.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(4)T	The **autosave** keyword was added.
12.4(7.20)T	The **retries** *number* and the **wait-time** *seconds* options were added.
12.4(11)T	This command was replaced with the **ip ips config location** command.

Usage Guidelines

When you specify the **ip ips sdf location** command, the signatures are not loaded until the router is rebooted or until the Intrusion Prevention System (IPS) is applied to an interface (through the **ip ips** command). If IPS is already applied to an interface, the signatures are not loaded. If IPS cannot load the SDF, an error message is issued and the router uses the built-in IPS signatures.

You can also specify the **copy ips-sdf** command to load an SDF from a specified location. Unlike the **ip ips sdf location** command, the signatures are loaded immediately after the **copy ips-sdf** command is entered.

When you specify the **autosave** keyword, the router saves a new SDF to the specified location when signatures are loaded using either the **copy** command or an external management platform such as Security Device Manager (SDM), IPS Management Center (IPSMC) or Cisco Incident Control Server (Cisco ICS). You can specify multiple autosave locations. The router will attempt to save to all autosave locations. The URL must have proper write access permissions.

Examples

The following example shows how to configure the router to load and merge the attack-drop.sdf file with the default signatures. After the files are merged, it is recommended that you copy the merged signatures to a separate file. You can then reload the router (by entering the **reload** command) or reinitialize the router so that it recognizes the newly merged file (as shown the following example).

```
!
ip ips name MYIPS
!
interface GigabitEthernet0/1
 ip address 10.1.1.16 255.255.255.0
 ip ips MYIPS in
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
!
!
! Merge the flash-based SDF (attack-drop.sdf) with the built-in signatures.
copy disk2:attack-drop.sdf ips-sdf
! Save the newly merged signatures to a separate file.
copy ips-sdf disk2:my-signatures.sdf
!
! Configure the router to use the new file, my-signatures.sdf
configure terminal
ip ips sdf location disk2:my-signatures.sdf
! Reinitialize the IPS by removing the IPS rule set and reapplying the rule set.
interface gig 0/1
no ip ips MYIPS in
!
*Apr 8 14:05:38.243:%IPS-2-DISABLED:IPS removed from all interfaces - IPS disabled
!
 ip ips MYIPS in
!
exit
```

Related Commands

Command	Description
copy ips-sdf	Loads or saves the SDF in the router.
ip ips	Applies the IPS rule to an interface.

ip ips signature

Note In Cisco IOS Release 12.4(11)T, the **ip ips signature** command was deprecated.

To attach a policy to a signature, use the **ip ips signature** command in global configuration mode. If the policy disabled a signature, use the **no** form of this command to reenable the signature. If the policy attached an access list to the signature, use the **no** form of this command to remove the access list.

ip ips signature *signature-id* {**delete** | **disable** | **list** *acl-list*}

no ip ips signature *signature-id*

Syntax Description

signature-id	Signature within the signature detection file (SDF).
delete	Deleted a specified signature.
disable	Disables a specified signature.
list *acl-list*	A named, standard, or ACL that is associated with the signature.

Defaults

No policy is attached to a signature.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	The command name was changed from the **ip audit signature** command to the **ip ips signature** command to support SDFs.
12.4(11)T	This command and support for SDFs were removed.

Usage Guidelines

This command allow you to set three policies: delete a signature, disable the audit of a signature, or qualify the audit of a signature with an access list.

If you are attaching an ACL to a signature, then you also need to create an Intrusion Prevention System (IPS) rule with the **ip ips name** command and apply it to an interface with the **ip ips** command.

Note The **ip ips signature** command replaces the **ip audit signature** command. If the **ip audit signature** command is found in an existing configuration, Cisco IOS IPS will interpret it as the **ip ips signature** command.

Examples

In the following example, a signature is disabled, another signature has ACL 99 attached to it, and ACL 99 is defined:

```
ip ips signature 6150 disable
ip ips signature 1000 list 99

access-list 99 deny 10.1.10.0 0.0.0.255
access-list 99 permit any
```

ip ips signature-category

To enter IPS category (config-ips-category) configuration mode, which allows you to tune Cisco IOS Intrusion Prevention System (IPS) signature parameters on the basis of a signature category, use the **ip ips signature-category** command in global configuration mode.

ip ips signature-category

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use the **ip ips signature-category** command if you want to tune signature parameters per category.

Examples

The following example shows how to tune event-action parameters for the signature category "adware/spyware." All tuning information will be applied to all signatures that belong to the adware/spyware category.

```
Router(config)# ip ips signature-category
Router(config-ips-category)# category attack adware/spyware
Router(config-ips-category-action)# event-action produce-alert
Router(config-ips-category-action)# event-action deny-packet-inline
Router(config-ips-category-action)# event-action reset-tcp-connection
Router(config-ips-category-action)# retired false
Router(config-ips-category-action)# ^Z
Do you want to accept these changes? [confirm]y
```

Related Commands

Command	Description
category	Specifies a signature category that is to be used for multiple signature actions or conditions.

ip ips signature-definition

To enter signature-definition-signature configuration mode, which allows you to define a signature for command-line interface (CLI) user tunings, use the **ip ips signature-definition** command in global configuration mode. To revert back to the default value, use the **no** form of this command.

ip ips signature-definition

no ip ips signature-definition

Syntax Description

This command has no arguments or keywords.

Command Default

Signature parameters cannot be defined and default values are used.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use the **ip ips signature-definition** command to enter signature-definition-signature configuration mode, which allows you to issue the **signature** command. The **signature** command is used to specify a signature whose CLI user tunings are to be customized. After you issue the **signature** command, you can begin to specify which signature parameters (user tunings) are to be changed.

Examples

The following example shows how to modify signature 5081/0 to “produce alert” and “reset tcp connection”:

```
Router(config)# ip ips signature-definition
Router(config-sigdef-sig)# signature 5081 0
Router(config-sigdef-action)# engine
Router(config-sigdef-action-engine)# event-action produce-alert reset-tcp-connection
Router(config-sigdef-action-engine)# ^Z
Do you want to accept these changes:[confirmm]y
```

Related Commands

Command	Description
signature	Specifies a signature for which the CLI user tunings will be changed.

ip ips signature disable

To instruct the router to scan for a given signature but not take any action if the signature is detected, use the **ip ips signature** command in global configuration mode. To reenable a signature, use the **no** form of this command.

ip ips signature *signature-id* [*sub-signature-id*] **disable** [**list** *acl-list*]

no ip ips signature *signature-id* [*sub-signature-id*] **disable** [**list** *acl-list*]

Syntax Description

signature-id [*sub-signature-id*]	Signature that is disabled.
list *acl-list*	(Optional) A named, standard, or extended access control list (ACL) to filter the traffic that will be scanned. If the packet is permitted by the ACL, the signature will be scanned and reported; if the packet is denied by the ACL, the signature is deemed disabled.

Defaults

All signatures within the signature definition file (SDF) are reported, if detected.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

You may want to disable a signature (or set of signatures) if your deployment scenario deems the signatures unnecessary.

Examples

The following example shows how to instructs the router not to report on signature 1000, if detected:

```
Router(config) ip ips signature 1000 disable
```

Related Commands

Command	Description
ip ips	Applies the IPS rule to an interface.
ip ips name	Specifies an IPS rule.

ip kerberos source-interface

To specify an interface for the source address of the kerberos packets, use the **ip kerberos source-interface** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ip kerberos source-interface *interface-type number*

no ip kerberos source-interface

Syntax Description

interface-type	Interface type. For more information, use the question mark (?) online help function.
number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Default

An interface for the source address of Kerberos packets is not set.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows how to specify an interface for the source address of the Kerberos packets:

```
Router# configure terminal
Router(config)# ip kerberos source-interface FastEthernet 0/0
```

Related Commands

Command	Description
clear kerberos creds	Deletes the contents of the credentials cache.
debug kerberos	Displays information associated with the Kerberos Authentication Subsystem.

ip msdp border

To configure a router that borders a Protocol Independent Multicast (PIM) sparse mode region and dense mode region to use Multicast Source Discovery Protocol (MSDP), use the **ip msdp border** command in global configuration mode. To prevent this action, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **border sa-address** *interface-type interface-number*

no ip msdp [**vrf** *vrf-name*] **border sa-address** *interface-type interface-number*

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
sa-address	Specifies the active source IP address.
interface-type interface-number	Interface type and number from which the IP address is derived and used as the rendezvous point (RP) address in Source-Active (SA) messages. Thus, MSDP peers can forward SA messages away from this border. The IP address of the interface is used as the originator ID, which is the RP field in the MSDP SA message. No space is needed between the values.

Defaults

The active sources in the dense mode region will not participate in MSDP.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command if you want the router to send SA messages for sources active in the PIM dense mode region to MSDP peers.

Specifying the interface-type and interface-number values allow the MSDP peers to forward source-active messages away from this border. The IP address of the interface is used as the originator ID, which is the rendezvous point field in the MSDP source-active message.

Note We recommend configuring the border router in the sparse mode domain to proxy-register sources in the dense mode domain, and have the sparse mode domain use standard MSDP procedures to advertise these sources.

Note If you use this command, you must constrain the sources advertised by using the **ip msdp redistribute** command. Configure the **ip msdp redistribute** command to apply to only local sources. Be aware that this configuration can result in (S, G) state remaining long after a source in the dense mode domain has stopped sending.

Note The **ip msdp originator-id** command also identifies an interface type and number to be used as the RP address. If both the **ip msdp border** and **ip msdp originator-id** commands are configured, the address derived from the **ip msdp originator-id** command determines the address of the RP.

Examples

In the following example, the local router is not an RP. It borders a PIM sparse mode region with a dense mode region. It uses the IP address of Ethernet interface 0 as the "RP" address in SA messages.

```
ip msdp border sa-address ethernet0
```

Related Commands

Command	Description
ip msdp originator-id	Allows an MSDP speaker that originates an SA message to use the IP address of its interface as the RP address in the SA message.
ip msdp redistribute	Configures which (S, G) entries from the multicast routing table are advertised in SA messages originated to MSDP peers.

ip mtu

To set the maximum transmission unit (MTU) size of IP packets that are sent on an interface, use the **ip mtu** command in interface configuration mode. To restore the default MTU size, use the **no** form of this command.

ip mtu *bytes*

no ip mtu

Syntax Description

bytes	MTU, in bytes.

Command Default

The IP MTU default value depends on the interface medium. Table 38 lists default MTU values according to media type.

Table 38 Default Media MTU Values

Media Type	Default MTU (Bytes)
Ethernet	1500
Serial	1500
Token Ring	4464
ATM	4470
FDDI	4470
HSSI (HSA)	4470
VASI	9216

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.

Usage Guidelines

If an IP packet exceeds the MTU that is set for the interface, the Cisco IOS software will fragment it.

For VASI interfaces that involve Ethernet type interfaces (Ethernet, Fast Ethernet or Gigabit Ethernet), the IP MTU of the VASI interface must be set the same as the lower default setting of the Ethernet type interface of 1500 bytes. If this adjustment is not made, OSPF reconvergence on the VASI interface will take too long.

Note Changing the MTU value (with the **mtu** interface configuration command) can affect the IP MTU value. If the current IP MTU value is the same as the MTU value, and you change the MTU value, the IP MTU value will be modified automatically to match the new MTU. However, the reverse is not true; changing the IP MTU value has no effect on the value for the **mtu** command.

Examples

The following example sets the maximum IP packet size for the first serial interface to 300 bytes:

```
Router(config)# interface serial 0
Router(config-if)# ip mtu 300
```

Related Commands

Command	Description
mtu	Adjusts the maximum packet size or MTU size.

ip nhrp cache non-authoritative

To turn off authoritative flags on NHRP cache entries, use the **ip nhrp cache non-authoritative** command in interface configuration mode. To turn authoritative flags on again, use the **no** form of this command.

ip nhrp cache non-authoritative

no ip nhrp cache non-authoritative

Syntax Description

This command has no arguments or keywords.

Defaults

Authoritative flags are turned on.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

By default the next hop server (NHS) replies to authoritative Next Hop Resolution Protocol (NHRP) resolution requests if it has a cache entry that is marked as authoritative. The **ip nhrp cache non-authoritative** comand turns off the "authoritative" flag on the cache entries. Thus, the request is forwarded to the next hop client (NHC), which responds to the resolution.

Configuring the **ip nhrp cache non-authoritative** command offloads the resolution replies from the hub to the spokes. It also helps the spokes complete NHRP mapping entries when a spoke-to-spoke tunnel is built, thus alleviating flap conditions in which the IP security (IPsec) tunnel is built but for which there are no corresponding NHRP mappings.

Examples

The following example shows that the authoritative flags have been turned off:

```
interface Tunnel0
 ip nhrp cache non-authoritative
```

ip nhrp nhs

To specify the address of one or more Next Hop Resolution Protocol (NHRP) servers, use the **ip nhrp nhs** command in interface configuration mode. To remove the address, use the **no** form of this command.

Cisco IOS Release 12.2(33)SRA, 12.2SX, and Later Releases

ip nhrp nhs *nhs-address* [*net-address* [*netmask*]]

no ip nhrp nhs *nhs-address* [*net-address* [*netmask*]]

Cisco IOS Release 15.1(2)T and Later Releases

ip nhrp nhs {*nhs-address* [**nbma** {*nbma-address* | *FQDN-string*}] [**multicast**] [**priority** *value*] [**cluster** *value*] | **cluster** *value* **max-connections** *value* | **dynamic nbma** {*nbma-address* | *FQDN-string*} [**multicast**] [**priority** *value*] [**cluster** *value*] | **fallback** *seconds*}

no ip nhrp nhs {*nhs-address* [**nbma** {*nbma-address* | *FQDN-string*}] [**multicast**] [**priority** *value*] [**cluster** *value*] | **cluster** *value* **max-connections** *value* | **dynamic nbma** {*nbma-address* | *FQDN-string*} [**multicast**] [**priority** *value*] [**cluster** *value*] | **fallback** *seconds*}

Syntax Description

nhs-address	Address of the next-hop server being specified.
net-address	(Optional) IP address of a network served by the next-hop server.
netmask	(Optional) IP network mask to be associated with the IP address. The IP address is logically ANDed with the mask.
nbma	(Optional) Specifies the nonbroadcast multiple access (NBMA) address or FQDN.
nbma-address	NBMA address.
FQDN-string	Next hop server (NHS) fully qualified domain name (FQDN) string.
multicast	(Optional) Specifies to use NBMA mapping for broadcasts and multicasts.
priority *value*	(Optional) Assigns a priority to hubs to control the order in which spokes select hubs to establish tunnels. The range is from 0 to 255; 0 is the highest and 255 is the lowest priority.
cluster *value*	(Optional) Specifies NHS groups. The range is from 0 to 10; 0 is the highest and 10 is the lowest. The default value is 0.
max-connections *value*	Specifies the number of NHS elements from each NHS group that needs to be active. The range is from 0 to 255.
dynamic	Configures the spoke to learn the NHS protocol address dynamically.
fallback *seconds*	Specifies the duration, in seconds, for which the spoke must wait before falling back to an NHS of higher priority upon recovery.

Defaults

No next-hop servers are explicitly configured, so normal network layer routing decisions are used to forward NHRP traffic.

Command Modes Interface configuration (config-if)

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(2)T	This command was modified. The *net-address* and *mask* arguments were removed and the **nbma**, *nbma-address*, *FQDN-string*, **multicast**, **priority** *value*, **cluster** *value*, **max-connections** *value*, **dynamic**, and **fallback** *seconds* keywords and arguments were added.

Usage Guidelines Use the **ip nhrp nhs** command to specify the address of a next hop server and the networks it serves. Normally, NHRP consults the network layer forwarding table to determine how to forward NHRP packets. When next hop servers are configured, these next hop addresses override the forwarding path that would otherwise be used for NHRP traffic.

For any next hop server that is configured, you can specify multiple networks by repeating this command with the same *nhs-address* argument, but with different IP network addresses.

Examples The following example shows how to register a hub to a spoke using NBMA and FQDN:

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ip nhrp nhs 192.0.2.1 nbma examplehub.example1.com
```

The following example shows how to configure the desired **max-connections** value:

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ip nhrp nhs cluster 5 max-connections 100
```

The following example shows how to configure the NHS fallback time:

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ip nhrp nhs fallback 25
```

The following example shows how to configure NHS priority and group values:

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ip nhrp nhs 192.0.2.1 priority 1 cluster 2
```

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
show ip nhrp	Displays NHRP mapping information.

ip port-map

To establish port-to-application mapping (PAM), use the **ip port-map** command in global configuration mode. To delete user-defined PAM entries, use the **no** form of this command.

ip port-map *appl-name* **port** [**tcp** | **udp**] [*port_num* | **from** *begin_port_num* **to** *end_port_num*] [**list** *acl-num*] [**description** *description_string*]

no ip port-map *appl-name* **port** [**tcp** | **udp**] [*port_num* | **from** *begin_port_num* **to** *end_port_num*] [**list** *acl-num*] [**description** *description_string*]

Syntax Description

appl-name	Specifies the name of the application with which to apply the port mapping. An application name can contain an underscore or a hyphen. An application can also be system or user-defined. However, a user-defined application must have the prefix **user-** in it; for example, **user-payroll**, **user-sales**, or **user-10**. Otherwise, the following error message appears: "Unable to add port-map entry. Names for user-defined applications must start with 'user-'."
port	Indicates that a port number maps to the application. You can specify up to five port numbers for each port.
tcp | **udp**	(Optional) Specifies the protocol for the application. For well-known applications (and those existing already under PAM), you can omit these keywords and the system assumes the standard protocol for that application. However, for user-defined applications, you must specify either **tcp** or **udp**.
port_num	(Optional) Identifies a port number in the range 1 to 65535.
from *begin_port_num* **to** *end_port_num*	(Optional) Specifies a range of port numbers. You must use the **from** and **to** keywords together.
list *acl-num*	(Optional) Indicates that the port mapping information applies to a specific host or subnet by associating it to an access control list (ACL) number used with PAM.
description *description_string*	(Optional) Specifies a description of up to 40 characters. **Note** Write the text string in the following format: "C *description_string* C," where "C" is a delimiting character.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(1)	Skinny Client Control Protocol (SCCP) support was added.

Release	Modification
12.3(14)T	Support was added for the following: • User-defined application names • User-specified descriptions • Port ranges • **tcp** and **udp** keywords • **from** *begin_port_num* **to** *end_port_num* keyword-argument combination • **description** *description_string* keyword-argument combination
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **ip port-map** command associates TCP or User Datagram Protocol (UDP) port numbers with applications or services, establishing a table of default port mapping information at the firewall. This information is used to support network environments that run services using ports that are different from the registered or well-known ports associated with a service or application.

When you issue the **no** form of the command, include all the parameters needed to remove the entry matching that specific set of parameters. For example, if you issued **no ip port-map** *appl-name*, then all entries for that application are removed.

The port mapping information in the PAM table is of one of three types:

- System-defined
- User-defined
- Host-specific

System-Defined Port Mapping

Initially, PAM creates a set of system-defined entries in the mapping table using well-known or registered port mapping information set up during the system start-up. The Cisco IOS Firewall Context-Based Access Control (CBAC) feature requires the system-defined port mapping information to function properly.

You can delete or modify system-defined port mapping information. Use the **no** form of the command for deletion and the regular form of the command to remap information to another application.

You can also add new port numbers to system-defined applications. However, for some system-defined applications like HTTP and Simple Mail Transfer Protocol (SMTP), in which the firewall inspects deeper into packets, their protocol (UDP or TCP) cannot be changed from that defined in the system. In those instances, error messages display.

Table 39 lists some default system-defined services and applications in the PAM table. (Use the **show ip port-map** command for the complete list.)

Table 39 System-Defined Port Mapping

Application Name	Well-Known or Registered Port Number	Protocol Description
cuseeme	7648	CU-SeeMe Protocol
exec	512	Remote Process Execution
ftp	21	File Transfer Protocol (control port)
h323	1720	H.323 Protocol (for example, MS NetMeeting, Intel Video Phone)
http	80	Hypertext Transfer Protocol
login	513	Remote login
msrpc	135	Microsoft Remote Procedure Call
netshow	1755	Microsoft NetShow
real-audio-video	7070	RealAudio and RealVideo
sccp	2000	Skinny Client Control Protocol (SCCP)
smtp	25	Simple Mail Transfer Protocol (SMTP)
sql-net	1521	SQL-NET
streamworks	1558	StreamWorks Protocol
sunrpc	111	SUN Remote Procedure Call
tftp	69	Trivial File Transfer Protocol
vdolive	7000	VDOLive Protocol

Note You can override system-defined entries for a specific host or subnet using the **list** *acl-num* option in the **ip port-map** command.

User-Defined Port Mapping

Network applications that use nonstandard ports require user-defined entries in the mapping table. Use the **ip port-map** command to create default user-defined entries in the PAM table. These entries automatically appear as an option for the **ip inspect name** command to facilitate the creation of inspection rules.

You can specify up to five separate port numbers for each port-map in a single entry. You can also specify a port range in a single entry. However, you may not specify both single port numbers and port ranges in the same entry.

Note If you try to map an application to a system-defined port, a message appears warning you of a mapping conflict. Delete the system-defined entry before mapping it to another application. Deleted system defined mappings appear in the running-configuration in their **no ip port-map** form.

Use the **no** form of the **ip port-map** command to delete user-defined entries from the PAM table. To remove a single mapping, use the **no** form of the command with all its parameters.

To overwrite an existing user-defined port mapping, use the **ip port-map** command to associate another service or application with the specific port.

Multiple commands for the same application name are cumulative.

If you assign the same port number to a new application, the new entry replaces the existing entry and it no longer appears in the running configuration. You receive a message about the remapping.

You cannot specify a port number that is in a range assigned to another application; however, you can specify a range that takes over one singly allocated port, or fully overlaps another range.

You cannot specify overlapping port ranges.

Host-Specific Port Mapping

User-defined entries in the mapping table can include host-specific mapping information, which establishes port mapping information for specific hosts or subnets. In some environments, it might be necessary to override the default port mapping information for a specific host or subnet, including a system-defined default port mapping information. Use the **list** *acl-num* option for the **ip port-map** command to specify an ACL for a host or subnet that uses PAM.

Note If the host-specific port mapping information is the same as existing system-defined or user-defined default entries, host-specific port changes have no effect.

Examples

The following example provides examples for adding and removing user-defined PAM configuration entries at the firewall.

In the following example, nonstandard port 8000 is established as the user-defined default port for HTTP services:

```
ip port-map http port 8000
```

The following example shows PAM entries that establish a range of nonstandard ports for HTTP services:

```
ip port-map http 8001
ip port-map http 8002
ip port-map http 8003
ip port-map http 8004
```

In the following example the command fails because it tries to map port 21, which is the system-defined default port for FTP, with HTTP:

```
ip port-map http port 21
```

In the following example, a specific host uses port 8000 for FTP services. ACL 10 identifies the server address (192.168.32.43), while port 8000 is mapped with FTP services:

```
access-list 10 permit 192.168.32.43
ip port-map ftp port 8000 list 10
```

In the following example, port 21, which is normally reserved for FTP services, is mapped to the RealAudio application for the hosts in list 10. In this configuration, hosts in list 10 do not recognize FTP activity on port 21.

```
ip port-map realaudio port 21 list 10
```

In the following example, the **ip port-map** command fails and generates an error message:

```
ip port-map netshow port 21
Command fail: the port 21 has already been defined for ftp by the system.
              No change can be made to the system defined port mappings.
```

In the following example, the **no** form of this command deletes user-defined entries from the PAM table. It has no effect on the system-defined port mappings. This command deletes the host-specific port mapping of FTP.

```
no ip port-map ftp port 1022 list 10
```

Note All **no** forms of the **ip port-map** command appear before other entries in the running configuration.

In the following example, the command fails because it tries to delete the system-defined default port for HTTP:

```
no ip port-map http port 80
```

In the following example, a specific host uses port 8000 for FTP services. ACL 10 identifies the server address (192.168.32.43), while port 8000 is mapped with FTP services.

```
access-list 10 permit 192.168.32.43
ip port-map ftp port 8000 list 10
```

In the following example, a specific subnet runs HTTP services on port 8080. ACL 50 identifies the subnet, while the PAM entry maps port 8080 with HTTP services.

```
access-list 50 permit 192.168.92.0
ip port-map http 8080 list 50
```

In the following example, a specific host runs HTTP services on port 25, which is the system-defined port number for SMTP services. This requires a host-specific PAM entry that overrides the system-defined default port mapping for HTTP, which is port 80. ACL 15 identifies the host address (192.168.33.43), while port 25 is mapped with HTTP services.

```
access-list 15 permit 192.168.33.43
ip port-map http port 25 list 15
```

In the following example, the same port number is required by different services running on different hosts. Port 8000 is required for HTTP services by host 192.168.3.4, while port 8000 is required for FTP services by host 192.168.5.6. ACL 10 and ACL 20 identify the specific hosts, while PAM maps the ports with the services for each ACL.

```
access-list 10 permit 192.168.3.4
access-list 20 permit 192.168.5.6
ip port-map http port 8000 list 10
ip port-map http ftp 8000 list 20
```

In the following example, five separate port numbers are specified:

```
ip port-map user-my-app port tcp 8085 8087 8092 8093 8094
```

In the following example, multiple commands for the same application name are cumulative and both ports map to the myapp application:

```
ip port-map user-myapp port tcp 3400
ip port-map user-myapp port tcp 3500
```

In the following example, the same port number is assigned to a new application. The new entry replaces the existing entry, meaning that port 5670 gets mapped to user-my-new-app and its mapping to myapp is removed. As a result, the first command no longer appears in the running configuration and you receive a message about the remapping.

```
ip port-map user-myapp port tcp 5670
ip port-map user-my-new-app port tcp 5670
```

In the following example, the second command assigns port 8085 to user-my-new-app because you cannot specify a port number that is in a range assigned to another application. As a result, the first command no longer appears in the running configuration, and you receive a message about the port being moved from one application to another.

```
ip port-map user-my-app port tcp 8085
ip port-map user-my-new-app port tcp from 8080 to 8090
```

Similarly, in the following example the second command assigns port range 8080 to 8085 to user-my-new-app and the first command no longer appears in the running configuration. You receive a message about the remapping.

```
ip port-map user-my-app port tcp from 8080 to 8085
ip port-map user-my-new-app port tcp from 8080 to 8090
```

Related Commands

Command	Description
show ip port-map	Displays the PAM information.

ip radius source-interface

To force RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets, use the **ip radius source-interface** command in global configuration mode. To prevent RADIUS from using the IP address of a specified interface for all outgoing RADIUS packets, use the **no** form of this command.

ip radius source-interface *subinterface-name* [**vrf** *vrf-name*]

no ip radius source-interface

Syntax Description

subinterface-name	Name of the interface that RADIUS uses for all of its outgoing packets.
vrf *vrf-name*	(Optional) Per virtual route forwarding (VRF) configuration.

Defaults

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3	This command was introduced.
12.2(1)DX	The **vrf** keyword and *vrf-name* argument were implemented on the Cisco 7200 series and Cisco 7401ASR.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use this command to set the IP address of a subinterface to be used as the source address for all outgoing RADIUS packets. The IP address is used as long as the subinterface is in the *up* state. The RADIUS server can use one IP address entry for every network access client instead of maintaining a list of IP addresses. Radius uses the IP address of the interface that it is associated to, regardless of whether the interface is in the *up* or *down* state.

The **ip radius source-interface**command is especially useful in cases where the router has many subinterfaces and you want to ensure that all RADIUS packets from a particular router have the same IP address.

If the specified subinterface does not have an IP address or is in the *down* state, then RADIUS reverts to the default. To avoid this, add an IP address to the subinterface or bring the subinterface to the *up* state.

Use the **vrf** *vrf-name* keyword and argument to configure this command per VRF, which allows multiple disjoined routing or forwarding tables, where the routes of one user have no correlation with the routes of another user.

Examples

The following example shows how to configure RADIUS to use the IP address of subinterface s2 for all outgoing RADIUS packets:

```
ip radius source-interface s2
```

The following example shows how to configure RADIUS to use the IP address of subinterface Ethernet0 for VRF definition:

```
ip radius source-interface Ethernet0 vrf vrf1
```

Related Commands

Command	Description
ip tacacs source-interface	Uses the IP address of a specified interface for all outgoing TACACS packets.
ip telnet source-interface	Allows a user to select an address of an interface as the source address for Telnet connections.
ip tftp source-interface	Allows a user to select the interface whose address will be used as the source address for TFTP connections.

ip reflexive-list timeout

To specify the length of time that reflexive access list entries will continue to exist when no packets in the session are detected, use the **ip reflexive-list timeout** command in global configuration mode. To reset the timeout period to the default timeout, use the **no** form of this command.

ip reflexive-list timeout *seconds*

no ip reflexive-list timeout

Syntax Description

seconds	Specifies the number of seconds to wait (when no session traffic is being detected) before temporary access list entries expire. Use a positive integer from 0 to 2,147,483. The default is 300 seconds.

Defaults

300 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is used with reflexive filtering, a form of session filtering.

This command specifies when a reflexive access list entry will be removed after a period of no traffic for the session (the timeout period).

With reflexive filtering, when an IP upper-layer session begins from within your network, a temporary entry is created within the reflexive access list, and a timer is set. Whenever a packet belonging to this session is forwarded (inbound or outbound) the timer is reset. When this timer counts down to zero without being reset, the temporary reflexive access list entry is removed.

The timer is set to the *timeout period*. Individual timeout periods can be defined for specific reflexive access lists, but for reflexive access lists that do not have individually defined timeout periods, the global timeout period is used. The global timeout value is 300 seconds by default; however, you can change the global timeout to a different value at any time using this command.

This command does not take effect for reflexive access list entries that were already created when the command is entered; this command only changes the timeout period for entries created after the command is entered.

Examples

The following example sets the global timeout period for reflexive access list entries to 120 seconds:

```
ip reflexive-list timeout 120
```

The following example returns the global timeout period to the default of 300 seconds:

```
no ip reflexive-list timeout
```

Related Commands

Command	Description
evaluate	Nests a reflexive access list within an access list.
ip access-list	Defines an IP access list by name.
permit (reflexive)	Creates a reflexive access list and enables its temporary entries to be automatically generated.

ip route (vasi)

To establish a static route on the VRF-Aware Service Infrastructure (VASI) interface, use the **ip route vrf** command in global configuration mode. To remove the static route connection, use the **no** form of this command.

ip route [**vrf** *vrf-name*] *destination-prefix detination-prefix-mask* {**vasileft** | **vasiright**} *number*

no ip route [**vrf** *vrf-name*] *destination-prefix detination-prefix-mask* {**vasileft** | **vasiright**} *number*

Syntax Description

vrf *vrf-name*	Specifies the Virtual Routing and Forwarding (VRF) instance for the static route.
destination-prefix	IP route prefix for the destination, in dotted decimal format.
destination-prefix-mask	Prefix mask for the destination, in dotted decimal format.
vasileft	Configures the vasileft interface.
vasiright	Configures the vasiright interface.
number	Identifier of the VASI interface. The range is from 1 to 256.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Examples

The following example shows how to configure static route on a VASI interface:

```
router(config)# ip route vrf red 0.0.0.0 0.0.0.0 vasileft 100
```

Related Commands

Command	Description
interface (vasi)	Configures the VASI interface.
debug interface (vasi)	Displays debugging information of VASI interface descriptor block.
debug vasi	Displays debugging information of VASI.
show vasi pair	Displays the status of a VASI pair.

ip scp server enable

To enable the router to securely copy files from a remote workstation, use the **ip scp server enable** command in global configuration mode. To disable secure copy functionality (the default), use the **no** form of this command.

ip scp server enable

no ip scp server enable

Syntax Description

This command has no arguments or keywords.

Defaults

The secure copy function is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)S	This command was integrated into Cisco IOS Release 12.0(21)S and support for the Cisco 7500 series and Cisco 12000 series routers was added.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(15)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

Use this command to enable secure copying of files from systems using the Secure Shell (SSH) application. This secure copy function is accomplished by an addition to the **copy** command in the Cisco IOS software, which takes care of using the secure copy protocol (scp) to copy to and from a router while logged in to the router itself. Because copying files is generally a restricted operation in the Cisco IOS software, a user attempting to copy such files needs to be at the correct enable level.

The Cisco IOS software must also allow files to be copied to or from itself from a remote workstation running the SSH application (which is supported by both the Microsoft Windows and UNIX operating systems). To get this information, the Cisco IOS software must have authentication and authorization configured in the authentication, authorization, and accounting (AAA) feature. SSH already relies on AAA authentication to authenticate the user username and password. Scp adds the requirement that AAA authorization be turned on so that the operating system can determine whether or not the user is at the correct privilege level.

Examples

The following example shows a typical configuration that allows the router to securely copy files from a remote workstation. Because scp relies on AAA authentication and authorization to function properly, AAA must be configured.

```
aaa new-model
aaa authentication login default tac-group tacacs+
aaa authorization exec default local
username user1 privilege 15 password 0 lab
ip scp server enable
```

The following example shows how to use scp to copy a system image from Flash memory to a server that supports SSH:

```
Router# copy flash:c4500-ik2s-mz.scp scp://user1@host1/

Address or name of remote host [host1]?
Destination username [user1]?
Destination filename [c4500-ik2s-mz.scp]?
Writing c4500-ik2s-mz.scp
Password:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Note When using scp, you cannot enter the password into the **copy** command; enter the password when prompted.

Related Commands

Command	Description
aaa authentication login	Sets AAA authentication at login.
aaa authorization	Sets parameters that restrict user access to a network.
copy	Copies any file from a source to a destination.
debug ip scp	Troubleshoots scp authentication problems.
ip ssh port	Enables secure network access to the tty lines.
username	Establishes a username-based authentication system.

ip sdee

To set the Security Device Event Exchange (SDEE) attribute values, use the **ip sdee** command in global configuration mode. To change the current selection or return to the default, use the **no** form of this command.

ip sdee {**alerts** *alert-number* | **messages** *message-number* | **subscriptions** *subscription-number*}

no ip sdee {**alerts** | **messages** | **subscriptions**}

Syntax Description

alerts *alert-number*	Specifies the maximum number of alerts the router must store. The range is from 10 to 2000. The default value is 200. **Note** Storing more alerts uses more router memory.
messages *message-number*	Specifies the maximum number of messages the router must store. The range is from 10 to 500. The default value is 200. **Note** Storing more messages uses more router memory.
subscriptions *subscription-number*	Specifies the maximum number of subscriptions. The range is from 1 to 3. The default value is 1.

Command Default

The default subscription is 1.
The default message is 200.
The default alert is 200.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **alerts** *alert-number* and **messages** *message-number* keywords and arguments were added.

Usage Guidelines

The SDEE messages report on the progress of Cisco IOS Intrusion Prevention System (IPS) initialization and operation. After you have enabled SDEE to receive and process events from IPS, you can issue the **ip sdee subscriptions** command to modify the number of allowed open SDEE subscriptions.

Examples

The following example shows how to change the number of allowed open subscriptions to 2:

```
Router# configure terminal
Router(config)# ip ips notify sdee
Router(config)# ip sdee events 500
Router(config)# ip sdee subscriptions 2
```

The following example shows how to change the number of alerts that must be stored on the router to 10:

```
Router# configure terminal
Router(config)# ip ips notify sdee
Router(config)# ip sdee events 500
Router(config)# ip sdee alerts 10
```

The following example shows how to change the number of messages that must be stored on the router to 10:

```
Router# configure terminal
Router(config)# ip ips notify sdee
Router(config)# ip sdee events 500
Router(config)# ip sdee messages 10
```

Related Commands

Command	Description
ip ips notify	Specifies the method of event notification.

ip sdee events

To set the maximum number of Security Device Event Exchange (SDEE) events that can be stored in the event buffer, use the **ip sdee events** command in global configuration mode. To change the buffer size or return to the default buffer size, use the **no** form of this command.

ip sdee events *events*

no ip sdee events *events*

Syntax Description

events	Maximum number of events; maximum number of allowable events: 1000.

Defaults

200 events

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

When SDEE notification is enabled (via the **ip ips notify sdee** command), 200 hundred events can automatically be stored in the buffer. When SDEE notification is disabled, all stored events are lost. A new buffer is allocated when the notifications are reenabled.

When specifying the size of an events buffer, note the following functionality:

- It is circular. When the end of the buffer is reached, the buffer will start overwriting the earliest stored events. (If overwritten events have not yet been reported, you will receive a buffer overflow notice.)
- If a new, smaller buffer is requested, all events that are stored in the previous buffer will be lost.
- If a new, larger buffer is requested, all existing events will be saved.

Examples

The following example shows how to set the maximum buffer events size to 500:

```
configure terminal
 ip ips notify sdee
 ip sdee events 500
```

Related Commands

Command	Description
ip ips notify	Specifies the method of event notification.

ip security add

To add a basic security option to all outgoing packets, use the **ip security add** command in interface configuration mode. To disable the adding of a basic security option to all outgoing packets, use the **no** form of this command.

ip security add

no ip security add

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled, when the security level of the interface is "Unclassified Genser" (or unconfigured). Otherwise, the default is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If an outgoing packet does not have a security option present, this interface configuration command will add one as the first IP option. The security label added to the option field is the label that was computed for this packet when it first entered the router. Because this action is performed after all the security tests have been passed, this label will either be the same or will fall within the range of the interface.

Examples

The following example adds a basic security option to each packet leaving Ethernet interface 0:

```
interface ethernet 0
 ip security add
```

Related Commands

Command	Description
ip security dedicated	Sets the level of classification and authority on the interface.
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.
ip security first	Prioritizes the presence of security options on a packet.
ip security ignore-authorities	Causes the Cisco IOS software to ignore the authorities field of all incoming packets.

Command	Description
ip security implicit-labelling	Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.
ip security multilevel	Sets the range of classifications and authorities on an interface.
ip security reserved-allowed	Treats as valid any packets that have Reserved1 through Reserved4 security levels.
ip security strip	Removes any basic security option on outgoing packets on an interface.

ip security aeso

To attach Auxiliary Extended Security Options (AESOs) to an interface, use the **ip security aeso** command in interface configuration mode. To disable AESO on an interface, use the **no** form of this command.

ip security aeso *source compartment-bits*

no ip security aeso *source compartment-bits*

Syntax Description

source	Extended Security Option (ESO) source. This can be an integer from 0 to 255.
compartment-bits	Number of compartment bits in hexadecimal.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Compartment bits are specified only if this AESO is to be inserted in a packet. On every incoming packet at this level on this interface, these AESOs should be present.

Beyond being recognized, no further processing of AESO information is performed. AESO contents are not checked and are assumed to be valid if the source is listed in the configurable AESO table.

Configuring any per-interface extended IP Security Option (IPSO) information automatically enables **ip security extended-allowed** (disabled by default).

Examples

The following example defines the Extended Security Option source as 5 and sets the compartments bits to 5:

```
interface ethernet 0
 ip security aeso 5 5
```

Related Commands

Command	Description
ip security eso-info	Configures system-wide defaults for extended IPSO information.
ip security eso-max	Specifies the maximum sensitivity level for an interface.

Command	Description
ip security eso-min	Configures the minimum sensitivity level for an interface.
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.

ip security dedicated

To set the level of classification and authority on the interface, use the **ip security dedicated** command in interface configuration mode. To reset the interface to the default classification and authorities, use the **no** form of this command.

ip security dedicated *level authority* [*authority...*]

no ip security dedicated *level authority* [*authority...*]

Syntax Description

level	Degree of sensitivity of information. The *level* keywords are listed in Table 40.
authority	Organization that defines the set of security levels that will be used in a network. The authority keywords are listed in Table 41.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

All traffic entering the system on this interface must have a security option that exactly matches this label. Any traffic leaving via this interface will have this label attached to it.

The following definitions apply to the descriptions of the IP Security Option (IPSO) in this section:

- level—The degree of sensitivity of information. For example, data marked TOPSECRET is more sensitive than data marked SECRET. The level keywords and their corresponding bit patterns are shown in Table 40.

Table 40 IPSO Level Keywords and Bit Patterns

Level Keyword	Bit Pattern
Reserved4	0000 0001
TopSecret	0011 1101
Secret	0101 1010
Confidential	1001 0110
Reserved3	0110 0110

Table 40 IPSO Level Keywords and Bit Patterns (continued)

Level Keyword	Bit Pattern
Reserved2	1100 1100
Unclassified	1010 1011
Reserved1	1111 0001

- authority—An organization that defines the set of security levels that will be used in a network. For example, the Genser authority consists of level names defined by the U.S. Defense Communications Agency (DCA). The authority keywords and their corresponding bit patterns are shown in Table 41.

Table 41 IPSO Authority Keywords and Bit Patterns

Authority Keyword	Bit Pattern
Genser	1000 0000
Siop-Esi	0100 0000
DIA	0010 0000
NSA	0001 0000
DOE	0000 1000

- label—A combination of a security level and an authority or authorities.

Examples

The following example sets a confidential level with Genser authority:

```
ip security dedicated confidential Genser
```

Related Commands

Command	Description
ip security add	Adds a basic security option to all outgoing packets.
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.
ip security first	Prioritizes the presence of security options on a packet.
ip security ignore-authorities	Causes the Cisco IOS software to ignore the authorities field of all incoming packets.
ip security implicit-labelling	Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.
ip security multilevel	Sets the range of classifications and authorities on an interface.
ip security reserved-allowed	Treats as valid any packets that have Reserved1 through Reserved4 security levels.
ip security strip	Removes any basic security option on outgoing packets on an interface.

ip security eso-info

To configure system-wide defaults for extended IP Security Option (IPSO) information, use the **ip security eso-info** command in global configuration mode. To return to the default settings, use the **no** form of this command.

ip security eso-info *source compartment-size default-bit*

no ip security eso-info *source compartment-size default-bit*

Syntax Description

source	Hexadecimal or decimal value representing the extended IPSO source. This is an integer from 0 to 255.
compartment-size	Maximum number of bytes of compartment information allowed for a particular extended IPSO source. This is an integer from 1 to 16.
default-bit	Default bit value for any unsent compartment bits.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command configures Extended Security Option (ESO) information, including Auxiliary Extended Security Option (AESO). Transmitted compartment information is padded to the size specified by the *compartment-size* argument.

Examples

The following example sets system-wide defaults for source, compartment size, and the default bit value:

```
ip security eso-info 100 5 1
```

Related Commands

Command	Description
ip security eso-max	Specifies the maximum sensitivity level for an interface.
ip security eso-min	Configures the minimum sensitivity level for an interface.

ip security eso-max

To specify the maximum sensitivity level for an interface, use the **ip security eso-max** command in interface configuration mode. To return to the default, use the **no** form of this command.

ip security eso-max *source compartment-bits*

no ip security eso-max *source compartment-bits*

Syntax Description

source	Extended Security Option (ESO) source. This is an integer from 1 to 255.
compartment-bits	Number of compartment bits in hexadecimal.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The command is used to specify the maximum sensitivity level for a particular interface. Before the per-interface compartment information for a particular Network-Level Extended Security Option (NLESO) source can be configured, the **ip security eso-info** global configuration command must be used to specify the default information.

On every incoming packet on the interface, these Extended Security Options should be present at the minimum level and should match the configured compartment bits. Every outgoing packet must have these ESOs.

On every packet transmitted or received on this interface, any NLESO sources present in the IP header should be bounded by the minimum sensitivity level and bounded by the maximum sensitivity level configured for the interface.

When transmitting locally generated traffic out this interface, or adding security information (with the **ip security add** command), the maximum compartment bit information can be used to construct the NLESO sources placed in the IP header.

A maximum of 16 NLESO sources can be configured per interface. Due to IP header length restrictions, a maximum of 9 of these NLESO sources appear in the IP header of a packet.

Examples

In the following example, the specified ESO source is 240 and the compartment bits are specified as 500:

```
interface ethernet 0
 ip security eso-max 240 500
```

Related Commands

Command	Description
ip security eso-info	Configures system-wide defaults for extended IPSO information.
ip security eso-min	Configures the minimum sensitivity level for an interface.

ip security eso-min

To configure the minimum sensitivity for an interface, use the **ip security eso-min** command in interface configuration mode. To return to the default, use the **no** form of this command.

ip security eso-min *source compartment-bits*

no ip security eso-min *source compartment-bits*

Syntax Description

source	Extended Security Option (ESO) source. This is an integer from 1 to 255.
compartment-bits	Number of compartment bits in hexadecimal.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The command is used to specify the minimum sensitivity level for a particular interface. Before the per-interface compartment information for a particular Network Level Extended Security Option (NLESO) source can be configured, the **ip security eso-info** global configuration command must be used to specify the default information.

On every incoming packet on this interface, these Extended Security Options should be present at the minimum level and should match the configured compartment bits. Every outgoing packet must have these ESOs.

On every packet transmitted or received on this interface, any NLESO sources present in the IP header should be bounded by the minimum sensitivity level and bounded by the maximum sensitivity level configured for the interface.

When transmitting locally generated traffic out this interface, or adding security information (with the **ip security add** command), the maximum compartment bit information can be used to construct the NLESO sources placed in the IP header.

A maximum of 16 NLESO sources can be configured per interface. Due to IP header length restrictions, a maximum of 9 of these NLESO sources appear in the IP header of a packet.

Examples

In the following example, the specified ESO source is 5, and the compartment bits are specified as 5:

```
interface ethernet 0
 ip security eso-min 5 5
```

Related Commands

Command	Description
ip security eso-info	Configures system-wide defaults for extended IPSO information.
ip security eso-max	Specifies the maximum sensitivity level for an interface.

ip security extended-allowed

To accept packets on an interface that has an extended security option present, use the **ip security extended-allowed** command in interface configuration mode. To restore the default, use the **no** form of this command.

ip security extended-allowed

no ip security extended-allowed

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Packets containing extended security options are rejected.

Examples

The following example allows interface Ethernet 0 to accept packets that have an extended security option present:

```
interface ethernet 0
 ip security extended-allowed
```

Related Commands

Command	Description
ip security add	Adds a basic security option to all outgoing packets.
ip security dedicated	Sets the level of classification and authority on the interface.
ip security first	Prioritizes the presence of security options on a packet.
ip security ignore-authorities	Causes the Cisco IOS software to ignore the authorities field of all incoming packets.
ip security implicit-labelling	Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.
ip security multilevel	Sets the range of classifications and authorities on an interface.

Command	Description
ip security reserved-allowed	Treats as valid any packets that have Reserved1 through Reserved4 security levels.
ip security strip	Removes any basic security option on outgoing packets on an interface.

ip security first

To prioritize the presence of security options on a packet, use the **ip security first** command in interface configuration mode. To prevent packets that include security options from moving to the front of the options field, use the **no** form of this command.

ip security first

no ip security first

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If a basic security option is present on an outgoing packet, but it is not the first IP option, then the packet is moved to the front of the options field when this interface configuration command is used.

Examples

The following example ensures that, if a basic security option is present in the options field of a packet exiting interface Ethernet 0, the packet is moved to the front of the options field:

```
interface ethernet 0
 ip security first
```

Related Commands

Command	Description
ip security add	Adds a basic security option to all outgoing packets.
ip security dedicated	Sets the level of classification and authority on the interface.
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.
ip security ignore-authorities	Causes the Cisco IOS software to ignore the authorities field of all incoming packets.
ip security implicit-labelling	Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.

Command	Description
ip security multilevel	Sets the range of classifications and authorities on an interface.
ip security reserved-allowed	Treats as valid any packets that have Reserved1 through Reserved4 security levels.
ip security strip	Removes any basic security option on outgoing packets on an interface.

ip security ignore-authorities

To have the Cisco IOS software ignore the authorities field of all incoming packets, use the **ip security ignore-authorities** command in interface configuration mode. To disable this function, use the **no** form of this command.

ip security ignore-authorities

no ip security ignore-authorities

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the packet's authority field is ignored, the value used in place of this field is the authority value declared for the specified interface. The **ip security ignore-authorities** can be configured only on interfaces that have dedicated security levels.

Examples

The following example causes interface Ethernet 0 to ignore the authorities field on all incoming packets:

```
interface ethernet 0
 ip security ignore-authorities
```

Related Commands

Command	Description
ip security add	Adds a basic security option to all outgoing packets.
ip security dedicated	Sets the level of classification and authority on the interface.
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.
ip security first	Prioritizes the presence of security options on a packet.
ip security implicit-labelling	Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.

Command	Description
ip security multilevel	Sets the range of classifications and authorities on an interface.
ip security reserved-allowed	Treats as valid any packets that have Reserved1 through Reserved4 security levels.
ip security strip	Removes any basic security option on outgoing packets on an interface.

ip security ignore-cipso

To enable Cisco IOS software to ignore the Commercial IP Security Option (CIPSO) field of all incoming packets at the interface, use the **ip security ignore-cipso** command in interface configuration mode. To disable this function, use the **no** form of this command.

ip security ignore-cipso

no ip security ignore-cipso

Syntax Description

This command has no arguments or keywords.

Command Default

Cisco IOS software cannot ignore the CIPSO field.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **ip security ignore-cipso** command allows a router running Cisco IOS software to ignore the CIPSO field in the IP packet and forward the packet as if the field was not present.

Examples

The following example shows how to enable Cisco IOS software to ignore the CIPSO field for all incoming packets at the Ethernet interface:

```
interface ethernet 0
 ip security ignore-cipso
```

The following sample output from the **show ip interface** command can be used to verify that the **ip security ignore-cipso** option has been enabled. If this option is enabled, the output will display the text “Commercial security options are ignored.”

```
Router# show ip interface ethernet 0

Ethernet0 is up, line protocol is up
Internet address is 172.16.0.0/28
Broadcast address is 255.255.255.255
Address determined by non-volatile memory
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is enabled
Secondary address 172.19.56.31/24
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
```

```
Commercial security options are ignored
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP multicast fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
Probe proxy name replies are disabled
Gateway Discovery is disabled
Policy routing is disabled
Network address translation is disabled
```

The following sample outputs from the **show ip traffic** command can be used to verify that the **ip security ignore-cipso** command has been enabled:

Sample Output Before the ip security ignore-cipso Command Was Introduced

```
Router# show ip traffic

IP statistics:
Rcvd: 153 total, 129 local destination
0 format errors, 0 checksum errors, 0 bad hop count
0 unknown protocol, 0 not a gateway
0 security failures, 34 bad options, 44 with options
Opts: 10 end, 0 nop, 0 basic security, 0 loose source route
0 timestamp, 0 extended security, 0 record route
0 stream ID, 0 strict source route, 0 alert, 0 other
Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
0 fragmented, 0 couldn't fragment
Bcast: 108 received, 1 sent
Mcast: 0 received, 4 sent
Sent: 30 generated, 0 forwarded
2 encapsulation failed, 0 no route
```

Sample Output with the ip security ignore-cipso Command Enabled

```
Router# show ip traffic

IP statistics:
Rcvd: 153 total, 129 local destination
0 format errors, 0 checksum errors, 0 bad hop count
0 unknown protocol, 0 not a gateway
0 security failures, 34 bad options, 44 with options
Opts: 10 end, 0 nop, 0 basic security, 0 loose source route
0 timestamp, 0 extended security, 0 record route
0 stream ID, 0 strict source route, 0 alert, 44 cipso
0 other
Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
0 fragmented, 0 couldn't fragment
Bcast: 108 received, 1 sent
Mcast: 0 received, 4 sent
Sent: 30 generated, 0 forwarded
2 encapsulation failed, 0 no route
```

Related Commands

Command	Description
show ip interfaces	Displays the usability status of interfaces configured for IP.
show ip traffic	Displays statistics about IP traffic.

ip security implicit-labelling

To force the Cisco IOS software to accept packets on the interface, even if they do not include a security option, use the **ip security implicit-labelling** command in interface configuration mode. To require security options, use the **no** form of this command.

ip security implicit-labelling [*level authority* [*authority...*]]

no ip security implicit-labelling [*level authority* [*authority...*]]

Syntax Description

level	(Optional) Degree of sensitivity of information. If your interface has multilevel security set, you must specify this argument. (See the *level* keywords listed in Table 40 in the **ip security dedicated** command section.)
authority	(Optional) Organization that defines the set of security levels that will be used in a network. If your interface has multilevel security set, you must specify this argument. You can specify more than one. (See the *authority* keywords listed in Table 41 in the **ip security dedicated** command section.)

Defaults

Enabled, when the security level of the interface is “Unclassified Genser” (or unconfigured). Otherwise, the default is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If your interface has multilevel security set, you must use the expanded form of the command (with the optional arguments as noted in brackets) because the arguments are used to specify the precise level and authority to use when labeling the packet. If your interface has dedicated security set, the additional arguments are ignored.

Examples

In the following example, an interface is set for security and will accept unlabeled packets:

```
ip security dedicated confidential genser
ip security implicit-labelling
```

Related Commands

Command	Description
ip security add	Adds a basic security option to all outgoing packets.
ip security dedicated	Sets the level of classification and authority on the interface.
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.
ip security first	Prioritizes the presence of security options on a packet.
ip security ignore-authorities	Causes the Cisco IOS software to ignore the authorities field of all incoming packets.
ip security multilevel	Sets the range of classifications and authorities on an interface.
ip security reserved-allowed	Treats as valid any packets that have Reserved1 through Reserved4 security levels.
ip security strip	Removes any basic security option on outgoing packets on an interface.

ip security multilevel

To set the range of classifications and authorities on an interface, use the **ip security multilevel** command in interface configuration mode. To remove security classifications and authorities, use the **no** form of this command.

ip security multilevel *level1* [*authority1...*] **to** *level2 authority2* [*authority2...*]

no ip security multilevel

Syntax Description

level1	Degree of sensitivity of information. The classification level of incoming packets must be equal to or greater than this value for processing to occur. (See the *level* keywords found in Table 40 in the **ip security dedicated** command section.)
authority1	(Optional) Organization that defines the set of security levels that will be used in a network. The authority bits must be a superset of this value. (See the *authority* keywords listed in Table 41 in the **ip security dedicated** command section.)
to	Separates the range of classifications and authorities.
level2	Degree of sensitivity of information. The classification level of incoming packets must be equal to or less than this value for processing to occur. (See the *level* keywords found in Table 40 in the **ip security dedicated** command section.)
authority2	Organization that defines the set of security levels that will be used in a network. The authority bits must be a proper subset of this value. (See the *authority* keywords listed in Table 41 in the **ip security dedicated** command section.)

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

All traffic entering or leaving the system must have a security option that falls within this range. Being within range requires that the following two conditions be met:

- The classification level must be greater than or equal to *level1* and less than or equal to *level2*.
- The authority bits must be a superset of *authority1* and a proper subset of *authority2*. That is, *authority1* specifies those authority bits that are required on a packet, and *authority2* specifies the required bits plus any optional authorities that also can be included. If the *authority1* field is the empty set, then a packet is required to specify any one or more of the authority bits in *authority2*.

Examples

The following example specifies levels Unclassified to Secret and NSA authority:

```
ip security multilevel unclassified to secret nsa
```

Related Commands

Command	Description
ip security add	Adds a basic security option to all outgoing packets.
ip security dedicated	Sets the level of classification and authority on the interface.
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.
ip security first	Prioritizes the presence of security options on a packet.
ip security ignore-authorities	Causes the Cisco IOS software to ignore the authorities field of all incoming packets.
ip security implicit-labelling	Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.
ip security reserved-allowed	Treats as valid any packets that have Reserved1 through Reserved4 security levels.
ip security strip	Removes any basic security option on outgoing packets on an interface.

ip security reserved-allowed

To treat as valid any packets that have Reserved1 through Reserved4 security levels, use the **ip security reserved-allowed** command in interface configuration mode. To disallow packets that have security levels of Reserved3 and Reserved2, use the **no** form of this command.

ip security reserved-allowed

no ip security reserved-allowed

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When you set multilevel security on an interface, and indicate, for example, that the highest range allowed is Confidential, and the lowest is Unclassified, the Cisco IOS software neither allows nor operates on packets that have security levels of Reserved3 and Reserved2 because they are undefined.

If you use the IP Security Option (IPSO) to block transmission out of unclassified interfaces, and you use one of the Reserved security levels, you *must* enable this feature to preserve network security.

Examples

The following example allows a security level of Reserved through Ethernet interface 0:

```
interface ethernet 0
 ip security reserved-allowed
```

Related Commands

Command	Description
ip security add	Adds a basic security option to all outgoing packets.
ip security dedicated	Sets the level of classification and authority on the interface.
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.
ip security first	Prioritizes the presence of security options on a packet.

Command	Description
ip security ignore-authorities	Causes the Cisco IOS software to ignore the authorities field of all incoming packets.
ip security implicit-labelling	Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.
ip security multilevel	Sets the range of classifications and authorities on an interface.
ip security strip	Removes any basic security option on outgoing packets on an interface.

ip security strip

To remove any basic security option on outgoing packets on an interface, use the **ip security strip** command in interface configuration mode. To restore security options, use the **no** form of this command.

ip security strip

no ip security strip

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The removal procedure is performed after all security tests in the router have been passed. This command is not allowed for multilevel interfaces.

Examples

The following example removes any basic security options on outgoing packets on Ethernet interface 0:

```
interface ethernet 0
 ip security strip
```

Related Commands

Command	Description
ip security add	Adds a basic security option to all outgoing packets.
ip security dedicated	Sets the level of classification and authority on the interface.
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.
ip security first	Prioritizes the presence of security options on a packet.
ip security ignore-authorities	Causes the Cisco IOS software to ignore the authorities field of all incoming packets.
ip security implicit-labelling	Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.

Command	Description
ip security multilevel	Sets the range of classifications and authorities on an interface.
ip security reserved-allowed	Treats as valid any packets that have Reserved1 through Reserved4 security levels.

ip source-track

To enable IP source tracking for a specified host, use the **ip source-track** command in global configuration mode. To disable IP source tracking, use the **no** form of this command.

ip source-track *ip-address*

no ip source-track *ip-address*

Syntax Description

ip-address	Destination IP address of the host that is to be tracked.

Defaults

IP address tracking is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(21)S	This command was introduced.
12.0(22)S	This command was implemented on the Cisco 7500 series routers.
12.0(26)S	This command was implemented on Cisco 12000 series ISE line cards.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

IP source tracking allows you to gather information about the traffic that is flowing to a host that is suspected of being under attack. It also allows you to easily trace a denial-of-service (DoS) attack to its entry point into the network.

After you have identified the destination that is being attacked, enable tracking for the destination address on the whole router by entering the **ip source-track** command.

Examples

The following example shows how to configure IP source tracking on all line cards and port adapters in the router. In this example, each line card or port adapter collects traffic flow data to host address 100.10.0.1 for 2 minutes before creating an internal system log entry; packet and flow information recorded in the system log is exported for viewing to the route processor or switch processor every 60 seconds.

```
Router# configure interface
Router(config)# ip source-track 10.10.0.1
Router(config)# ip source-track syslog-interval 2
Router(config)# ip source-track export-interval 60
```

Related Commands

Command	Description
ip source-track address-limit	Configures the maximum number of destination hosts that can be simultaneously tracked at any given moment.
ip source-track export-interval	Sets the time interval (in seconds) in which IP source tracking statistics are exported from the line card to the RP.
ip source-track syslog-interval	Sets the time interval (in minutes) in which syslog messages are generated if IP source tracking is enabled on a device.
show ip source-track	Displays traffic flow statistics for tracked IP host addresses.
show ip source-track export flows	Displays the last 10 packet flows that were exported from the line card to the route processor.

ip source-track address-limit

To configure the maximum number of destination hosts that can be simultaneously tracked at any given moment, use the **ip source-track address-limit** command in global configuration mode. To cancel this administrative limit and return to the default, use the **no** form of this command.

ip source-track address-limit *number*

no ip source-track address-limit *number*

Syntax Description

number	Maximum number of hosts that can be tracked.

Defaults

An unlimited number of hosts can be tracked.

Command Modes

Global configuration

Command History

Release	Modification
12.0(21)S	This command was introduced.
12.0(22)S	This command was implemented on the Cisco 7500 series routers.
12.0(26)S	This command was implemented on Cisco 12000 series ISE line cards.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

After you have configured at least one destination IP address for source tracking (via the **ip source-track** command), you can limit the number of destination IP addresses that can be tracked via the **ip source-track address-limit** command.

Examples

The following example shows how to configure IP source tracking for data that flows to host 100.10.1.1 and limit IP source tracking to 10 IP addresses:

```
Router(config)# ip source-track 100.10.0.1
Router(config)# ip source-track address-limit 10
```

Related Commands

Command	Description
ip source-track	Enables IP source tracking for a specified host.
show ip source-track	Displays traffic flow statistics for tracked IP host addresses.

ip source-track export-interval

To set the time interval (in seconds) in which IP source tracking statistics are exported from the line card to the route processor (RP), use the **ip source-track export-interval** command in global configuration mode. To return to default functionality, use the **no** form of this command.

ip source-track export-interval *number*

no ip source-track export-interval *number*

Syntax Description

number	Number of seconds that pass before IP source tracking statistics are exported.

Defaults

Traffic flow information is exported from the line card to the RP every 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.0(21)S	This command was introduced.
12.0(22)S	This command was implemented on the Cisco 7500 series routers.
12.0(26)S	This command was implemented on Cisco 12000 series ISE line cards.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ip source-track export-interval** command to specify the frequency in which IP source tracking information is sent to the RP for viewing.

Note This command can be issued only on distributed platforms such as the gigabit route processor (GRP) and the route switch processor (RSP).

Examples

The following example shows how to configure IP source tracking on all line cards and port adapters in the router. In this example, each line card or port adapter collects traffic flow data to host address 100.10.0.1 for 2 minutes before creating an internal system log entry; packet and flow information recorded in the system log is exported for viewing to the route processor or switch processor every 60 seconds.

```
Router# configure interface
```

```
Router(config)# ip source-track 10.10.0.1
Router(config)# ip source-track syslog-interval 2
Router(config)# ip source-track export-interval 60
```

Related Commands

Command	Description
ip source-track	Enables IP source tracking for a specified host.
show ip source-track export flows	Displays the last 10 packet flows that were exported from the line card to the route processor.

ip source-track syslog-interval

To set the time interval (in minutes) in which syslog messages are generated if IP source tracking is enabled on a device, use the **ip source-track syslog-interval** command in global configuration mode. To cancel this setting and disable syslog generation, use the **no** form of this command.

ip source-track syslog-interval *number*

no ip source-track syslog-interval *number*

Syntax Description

number	IP address of the destination that is to be tracked.

Defaults

Syslog messages are not generated.

Command Modes

Global configuration

Command History

Release	Modification
12.0(21)S	This command was introduced.
12.0(22)S	This command was implemented on the Cisco 7500 series routers.
12.0(26)S	This command was implemented on Cisco 12000 series ISE line cards.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ip source-track syslog-interval** command to track the source interfaces of traffic that are destined to a particular address.

Examples

The following example shows how to configure IP source tracking on all line cards and port adapters in the router. In this example, each line card or port adapter collects traffic flow data to host address 100.10.0.1 for 2 minutes before creating an internal system log entry; packet and flow information recorded in the system log is exported for viewing to the route processor or switch processor every 60 seconds.

```
Router# configure interface
Router(config)# ip source-track 10.10.0.1
Router(config)# ip source-track syslog-interval 2
Router(config)# ip source-track export-interval 60
```

Related Commands

Command	Description
ip source-track	Enables IP source tracking for a specified host.
show ip source-track	Displays traffic flow statistics for tracked IP host addresses.

ip ssh

To configure Secure Shell (SSH) control parameters on your router, use the **ip ssh** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip ssh [**timeout** *seconds* | **authentication-retries** *integer*]

no ip ssh [**timeout** *seconds* | **authentication-retries** *integer*]

Syntax Description

timeout	(Optional) The time interval that the router waits for the SSH client to respond. This setting applies to the SSH negotiation phase. Once the EXEC session starts, the standard timeouts configured for the vty apply. By default, there are 5 vtys defined (0–4), therefore 5 terminal sessions are possible. After the SSH executes a shell, the vty timeout starts. The vty timeout defaults to 10 minutes.
seconds	(Optional) The number of seconds until timeout disconnects, with a maximum of 120 seconds. The default is 120 seconds.
authentication-retries	(Optional) The number of attempts after which the interface is reset.
integer	(Optional) The number of retries, with a maximum of 5 authentication retries. The default is 3.

Command Default

SSH control parameters are set to default router values.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1) T.
12.2(17a)SX	This command was integrated into Cisco IOS Release 12.2(17a)SX.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

Before you configure SSH on your router, you must enable the SSH server using the **crypto key generate rsa** command.

Examples

The following examples configure SSH control parameters on your router:

```
ip ssh timeout 120
ip ssh authentication-retries 3
```

ip ssh break-string

To configure a string that, when received from a Secure Shell (SSH) client, will cause the Cisco IOS SSH server to transmit a break signal out an asynchronous line, use the **ip ssh break-string** command in global configuration mode. To remove the string, use the **no** form of this command.

ip ssh break-string *string*

no ip ssh break-string *string*

Syntax Description

string	Any sequence of characters not including embedded whitespace. Include control characters by prefixing them with ^V (control/V) or denote them using the \000 notation (that is, a backslash followed by the the ASCII value of the character in three octal digits.)

Defaults

Break signal is not enabled

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.

Usage Guidelines

Note This break string is used only for SSH sessions that are outbound on physical lines using the SSH Terminal-Line Access feature. This break string is not used by the Cisco IOS SSH client, nor is it used by the Cisco IOS SSH server when the server uses a virtual terminal (VTY) line. This break string does not provide any interoperability with the method that is described in the Internet Engineering Task Force (IETF) Internet-Draft “Session Channel Break Extension” (draft-ietf-secsh-break-02.txt).

Note In some versions of Cisco IOS, if the SSH break string is set to a single character, the Cisco IOS server will not immediately process that character as a break signal on receipt of that character but will delay until it has received a subsequent character. A break string of two or more characters will be immediately processed as a break signal after the last character in the string has been received from the SSH client.

Examples

The following example shows that the control-B character (ASCII 2) has been set as the SSH break string:

```
Router (config)# ip ssh break-string \002
```

Related Commands

Command	Description
ip ssh port	Enables SSH access to TTY lines.

ip ssh dh min size

To configure the modulus size on the Secure Shell (SSH) server, use the **ip ssh dh min size** command in privileged EXEC mode. To disable the configuration, use the **no** form of this command.

ip ssh dh min size [*number*]

no ip ssh dh min size

Syntax Description

number	(Optional) Minimum number of bits in the key size. The default is 1024.

Command Default

Bit key support is disabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.

Usage Guidelines

Use the **ip ssh dh min size** command to ensure that the CLI is successfully parsed from either the client side or the server side.

Examples

The following example shows how to set the minimum modulus size to 2048 bits:

```
Router> enable
Router# ip ssh dh min size 2048
```

Related Commands

Command	Description
show ip ssh	Displays the status of SSH server connections.

ip ssh dscp

To specify the IP differentiated services code point (DSCP) value that can be set for a Secure Shell (SSH) configuration, use the **ip ssh dscp** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip ssh dscp *number*

no ip ssh dscp *number*

Syntax Description

number	Value that can be set. The default value is 0 (zero). • *number*—0 through 63.

Command Default

The IP DSCP value is not specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)S	This command was introduced.
12.2SR	This command is supported in the Cisco IOS Release 12.2SR train. Support in a specific 12.2SR train depends on your feature set, platform, and platform hardware.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX train depends on your feature set, platform, and platform hardware.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

IP DSCP values can be configured on both the SSH client and the SSH server for SSH traffic that is generated on either end.

Examples

The following example shows that the DSCP value is set to 35:

```
Router(config)# ip ssh dscp 35
```

Related Commands

Command	Description
ip ssh precedence	Specifies the IP precedence value that may be set.

ip ssh maxstartups

To set the maximum concurrent sessions allowed on a Secure Shell (SSH), use the **ip ssh maxstartups** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ip ssh maxstartups [*number*]

no ip ssh maxstartups [*number*]

Syntax Description

number	(Optional) Number of connections to be accepted concurrently. The range is from 2 to 128. The default is 128.

Command Default

The number of maximum concurrent sessions is 128.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

You must create RSA keys to enable SSH. The RSA key must be at least 768 bits for SSHv2.

Examples

The following example shows how to set the maximum concurrent sessions allowed on a SSH to 100:

```
Router# configure terminal
Router(config)# ip ssh maxstartups 100
```

Related Commands

Command	Description
debug ip ssh	Displays debugging messages for SSH.
ip ssh	Configures SSH control parameters on your router.

ip ssh port

To enable secure access to tty (asynchronous) lines, use the **ip ssh port** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip ssh port *por-tnum* **rotary** *group*

no ip ssh port *por-tnum* **rotary** *group*

Syntax Description

port-num	Specifies the port, such as 2001, to which Secure Shell (SSH) needs to connect.
rotary *group*	Specifies the defined rotary that should search for a valid name.

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

The **ip ssh port** command supports a functionality that replaces reverse Telnet with SSH. Use this command to securely access the devices attached to the serial ports of a router and to perform the following tasks:

- Connect to a router with multiple terminal lines that are connected to consoles of other devices.
- Allow network available modems to be securely accessed for dial-out.

Examples

The following example shows how to configure the SSH Terminal-Line Access feature on a modem that is used for dial-out on lines 1 through 200:

```
line 1 200
 no exec
 login authentication default
 rotary 1
 transport input ssh

ip ssh port 2000 rotary 1
```

The following example shows how to configure the SSH Terminal-Line Access feature to access the console ports of various devices that are attached to the serial ports of the router. For this type of access, each line is put into its own rotary, and each rotary is used for a single port. In this example, lines 1 through 3 are used, and the port (line) mappings of the configuration are as follows: Port 2001 = Line 1, Port 2002 = Line 2, and Port 2003 = Line 3.

```
line 1
 no exec
 login authentication default
 rotary 1
 transport input ssh
line 2
 no exec
 login authentication default
 rotary 2
 transport input ssh
line 3
 no exec
 login authentication default
 rotary 3
 transport input ssh

ip ssh port 2001 rotary 1 3
```

From any UNIX or UNIX-like device, the following command is typically used to form an SSH session:

```
ssh -c 3des -p 2002 router.example.com
```

This command will initiate an SSH session using the Triple DES cipher to the device known as "router.example.com," which uses port 2002. This device will connect to the device on Line 2, which was associated with port 2002. Similarly, many Windows SSH packages have related methods of selecting the cipher and the port for this access.

Related Commands

Command	Description
crypto key generate rsa	Enables the SSH server.
debug ip ssh	Displays debugging messages for SSH.
ip ssh	Configures SSH control variables on your router.
line	Identifies a specific line for configuration and begins the command in line configuration mode.
rotary	Defines a group of lines consisting of one or more lines.
ssh	Starts an encrypted session with a remote networking device.
transport input	Defines which protocols to use to connect to a specific line of the router.

ip ssh precedence

To specify the IP precedence value that can be set for a Secure Shell (SSH) configuration, use the **ip ssh precedence** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip ssh precedence *number*

no ip ssh precedence *number*

Syntax Description

number	Value that can be set. The default value is 0 (zero). • *number*—0 through 7.

Command Default

The IP precedence value is not specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(20)S	This command was introduced.
12.2SR	This command is supported in the Cisco IOS Release 12.2SR train. Support in a specific 12.2SR train depends on your feature set, platform, and platform hardware.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX train depends on your feature set, platform, and platform hardware.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

IP precedence values can be configured on both the SSH client and the SSH server for SSH traffic that is generated on either end.

Examples

The following example shows that up to six IP precedence values can be set:

```
Router(config)# ip precedence value 6
```

Related Commands

Command	Description
ip ssh dscp	Specifies the IP DSCP value that can be set for an SSH configuration.

ip ssh pubkey-chain

To configure Secure Shell RSA (SSH-RSA) keys for user and server authentication on the SSH server, use the **ip ssh pubkey-chain** command in global configuration mode. To remove SSH-RSA keys for user and server authentication on the SSH server, use the **no** form of this command.

ip ssh pubkey-chain

no ip ssh pubkey-chain

Syntax Description

This command has no arguments or keywords.

Command Default

SSH-RSA keys are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines

Use the **ip ssh pubkey-chain** command to ensure SSH server and user public key authentication.

Examples

The following example shows how to enable public key generation:

```
Router(config)# ip ssh pubkey-chain
```

Related Commands

Command	Description
ip ssh stricthostkeycheck	Enables strict host key checking on the SSH server.

ip ssh rsa keypair-name

To specify which Rivest, Shimar, and Adelman (RSA) key pair to use for a Secure Shell (SSH) connection, use the **ip ssh rsa keypair-name** command in global configuration mode. To disable the key pair that was configured, use the **no** form of this command.

ip ssh rsa keypair-name *keypair-name*

no ip ssh rsa keypair-name *keypair-name*

Syntax Description

keypair-name	Name of the key pair.

Command Default

If this command is not configured, SSH will use the first RSA key pair that is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(7)JA	This command was integrated into Cisco IOS Release 12.3(7)JA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

Using the **ip ssh rsa keypair-name** command, you can enable an SSH connection using RSA keys that you have configured using the *keypair-name* argument. Previously, SSH was tied to the first RSA keys that were generated (that is, SSH was enabled when the first RSA key pair was generated). The previous behavior still exists, but by using the **ip ssh rsa keypair-name** command, you can overcome that behavior. If you configure the **ip ssh rsa keypair-name** command with a key pair name, SSH is enabled if the key pair exists, or SSH will be enabled if the key pair is generated later. If you use this command, you are not forced to configure a hostname and a domain name.

Note A Cisco IOS router can have many RSA key pairs.

Examples

The following example shows how to specify the RSA key pair "sshkeys" for an SSH connection:

```
Router# configure terminal
Router(config)# ip ssh rsa keypair-name sshkeys
```

Related Commands

Command	Description
debug ip ssh	Displays debug messages for SSH.
disconnect ssh	Terminates a SSH connection on your router.
ip ssh	Configures SSH control parameters on your router.
ip ssh version	Specifies the version of SSH to be run on a router.
show ip ssh	Displays the SSH connections of your router.

ip ssh source-interface

To specify the IP address of an interface as the source address for a Secure Shell (SSH) client device, use the **ip ssh source-interface** command in global configuration mode. To remove the IP address as the source address, use the **no** form of this command.

ip ssh source-interface *interface*

no ip ssh source-interface *interface*

Syntax Description

interface	The interface whose address is used as the source address for the SSH client.

Defaults

The address of the closest interface to the destination is used as the source address (the closest interface is the output interface through which the SSH packet is sent).

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

By specifying this command, you can force the SSH client to use the IP address of the source interface as the source address.

Examples

In the following example, the IP address assigned to Ethernet interface 0 will be used as the source address for the SSH client:

```
ip ssh source-interface ethernet0
```

ip ssh stricthostkeycheck

To enable strict host key checking on the Secure Shell (SSH) server, use the **ip ssh stricthostcheck** command in global configuration mode. To disable strict host key checking, use the **no** form of this command.

ip ssh stricthostkeycheck

no ip ssh stricthostkeycheck

Syntax Description

This command has no arguments or keywords.

Command Default

Strict host key checking on the SSH server is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines

Use the **ip ssh stricthostkeycheck** command to ensure SSH server side strict checking. Configuring the **ip ssh stricthostkeycheck** command authenticates all servers.

Note

- This command is not available on SSH Version 1.
- If the **ip ssh pubkey-chain** command is not configured, the **ip ssh stricthostkeycheck** command will lead to connection failure in SSH Version 2.

Examples

The following example shows how to enable strict host key checking:

```
Router(config)# ip ssh stricthostkeycheck
```

Related Commands

Command	Description
ip ssh pubkey-chain	Configures SSH-RSA keys for user and server authentication on the SSH server.

ip ssh version

To specify the version of Secure Shell (SSH) to be run on a router, use the **ip ssh version** command in global configuration mode. To disable the version of SSH that was configured and to return to compatibility mode, use the **no** form of this command.

ip ssh version [**1** | **2**]

no ip ssh version [**1** | **2**]

Syntax Description

1	(Optional) Router runs only SSH Version 1.
2	(Optional) Router runs only SSH Version 2.

Defaults

If this command is not configured, SSH operates in compatibility mode, that is, Version 1 and Version 2 are both supported.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(7)JA	This command was integrated into Cisco IOS Release 12.3(7)JA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

You can use this command with the **2** keyword to ensure that your router will not inadvertently establish a weaker SSH Version 1 connection.

Examples

The following example shows that only SSH Version 1 support is configured:

```
Router (config)# ip ssh version 1
```

The following example shows that only SSH Version 2 is configured:

```
Router (config)# ip ssh version 2
```

The following example shows that SSH Versions 1 and 2 are configured:

```
Router (config)# no ip ssh version
```

Related Commands

Command	Description
debug ip ssh	Displays debug messages for SSH.
disconnect ssh	Terminates a SSH connection on your router.
ip ssh	Configures SSH control parameters on your router.
ip ssh rsa keypair-name	Specifies which RSA key pair to use for a SSH connection.
show ip ssh	Displays the SSH connections of your router.

ip tacacs source-interface

To use the IP address of a specified interface for all outgoing TACACS+ packets, use the **ip tacacs source-interface** command in global configuration or server-group configuration mode. To disable use of the specified interface IP address, use the **no** form of this command.

ip tacacs source-interface *subinterface-name*

no ip tacacs source-interface

Syntax Description

subinterface-name	Name of the interface that TACACS+ uses for all of its outgoing packets.

Command Default

None

Command Modes

Global configuration (config)

Server-group configuration (server-group)

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	This command was introduced in server-group configuration mode.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(54)SG	This command was integrated into Cisco IOS Release 12.2(54)SG.

Usage Guidelines

Use this command to set the IP address of a subinterface for all outgoing TACACS+ packets. This address is used as long as the interface is in the *up* state. In this way, the TACACS+ server can use one IP address entry associated with the network access client instead of maintaining a list of all IP addresses.

This command is especially useful in cases where the router has many interfaces and you want to ensure that all TACACS+ packets from a particular router have the same IP address.

The specified interface must have an IP address associated with it. If the specified subinterface does not have an IP address or is in a *down* state, TACACS+ reverts to the default. To avoid this situation, add an IP address to the subinterface or bring the interface to the *up* state.

Note This command can be configured globally or in server-group configuration mode. If this command is configured in the server-group configuration mode, the IP address of the specified interface is used for packets that are going only to servers that are defined in that server group. If this command is not configured in server-group configuration mode, the global configuration applies.

Examples

The following example makes TACACS+ use the IP address of subinterface "s2" for all outgoing TACACS+ packets:

```
ip tacacs source-interface s2
```

In the following example, TACACS+ is to use the IP address of Loopback0 for packets that are going only to server 10.1.1.1:

```
aaa group server tacacs+ tacacs1
    server-private 10.1.1.1 port 19 key cisco
    ip vrf forwarding cisco
    ip tacacs source-interface Loopback0

  ip vrf cisco
   rd 100:1

  interface Loopback0
   ip address 10.0.0.2 255.0.0.0
   ip vrf forwarding cisco
```

Related Commands

Command	Description
ip radius source-interface	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.
ip telnet source-interface	Allows a user to select an address of an interface as the source address for Telnet connections.
ip tftp source-interface	Allows a user to select the interface whose address will be used as the source address for TFTP connections.
ip vrf forwarding (server-group)	Configures the VRF reference of an AAA RADIUS or TACACS+ server group.
server-private	Configures the IP address of the private RADIUS or TACACS+ server for the group server.

ip tcp intercept connection-timeout

To change how long a TCP connection will be managed by the TCP intercept after no activity, use the **ip tcp intercept connection-timeout** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept connection-timeout *seconds*

no ip tcp intercept connection-timeout [*seconds*]

Syntax Description

seconds	Time (in seconds) that the software will still manage the connection after no activity. The minimum value is 1 second. The default is 86,400 seconds (24 hours).

Defaults

86,400 seconds (24 hours)

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ip tcp intercept connection-timeout** command to change how long a TCP connection will be managed by the TCP intercept after a period of inactivity.

Examples

The following example sets the software to manage the connection for 12 hours (43,200 seconds) after no activity:

```
ip tcp intercept connection-timeout 43200
```

ip tcp intercept drop-mode

To set the TCP intercept drop mode, use the **ip tcp intercept drop-mode** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept drop-mode [**oldest | random**]

no ip tcp intercept drop-mode [**oldest | random**]

Syntax Description

oldest	(Optional) Software drops the oldest partial connection. This is the default.
random	(Optional) Software drops a randomly selected partial connection.

Defaults

oldest

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the number of incomplete connections exceeds 1100 or the number of connections arriving in the last 1 minute exceeds 1100, the TCP intercept feature becomes more aggressive. When this happens, each new arriving connection causes the oldest partial connection to be deleted, and the initial retransmission timeout is reduced by half to 0.5 seconds (and so the total time trying to establish the connection will be cut in half).

Note that the 1100 thresholds can be configured with the **ip tcp intercept max-incomplete high** and **ip tcp intercept one-minute high** commands.

Use the **ip tcp intercept drop-mode** command to change the dropping strategy from oldest to a random drop.

Examples

The following example sets the drop mode to random:

```
ip tcp intercept drop-mode random
```

Related Commands

Command	Description
ip tcp intercept max-incomplete high	Defines the maximum number of incomplete connections allowed before the software enters aggressive mode.
ip tcp intercept max-incomplete low	Defines the number of incomplete connections below which the software leaves aggressive mode.
ip tcp intercept one-minute high	Defines the number of connection requests received in the last one-minute sample period before the software enters aggressive mode.
ip tcp intercept one-minute low	Defines the number of connection requests below which the software leaves aggressive mode.

ip tcp intercept finrst-timeout

To change how long after receipt of a reset or FIN-exchange the software ceases to manage the connection, use the **ip tcp intercept finrst-timeout** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept finrst-timeout *seconds*

no ip tcp intercept finrst-timeout [*seconds*]

Syntax Description

seconds	Time (in seconds) after receiving a reset or FIN-exchange that the software ceases to manage the connection. The minimum value is 1 second. The default is 5 seconds.

Defaults

5 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Even after the two ends of the connection are joined, the software intercepts packets being sent back and forth. Use this command if you need to adjust how soon after receiving a reset or FIN-exchange the software stops intercepting packets.

Examples

The following example sets the software to wait for 10 seconds before it leaves intercept mode:

```
ip tcp intercept finrst-timeout 10
```

ip tcp intercept list

To enable TCP intercept, use the **ip tcp intercept list** command in global configuration mode. To disable TCP intercept, use the **no** form of this command.

ip tcp intercept list *access-list-number*

no ip tcp intercept list *access-list-number*

Syntax Description

access-list-number	Extended access list number in the range from 100 to 199.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The TCP intercept feature intercepts TCP connection attempts and shields servers from TCP SYN-flood attacks, also known as denial-of-service attacks.

TCP packets matching the access list are presented to the TCP intercept code for processing, as determined by the **ip tcp intercept mode** command. The TCP intercept code either intercepts or watches the connections.

To have all TCP connection attempts submitted to the TCP intercept code, have the access list match everything.

Examples

The following example configuration defines access list 101, causing the software to intercept packets for all TCP servers on the 192.168.1.0/24 subnet:

```
ip tcp intercept list 101
!
access-list 101 permit tcp any 192.168.1.0 0.0.0.255
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
ip tcp intercept mode	Changes the TCP intercept mode.

Command	Description
show tcp intercept connections	Displays TCP incomplete and established connections.
show tcp intercept statistics	Displays TCP intercept statistics.

ip tcp intercept max-incomplete

To define either the number of incomplete connections below which the software leaves aggressive mode or the maximum number of incomplete connections allowed before the software enters aggressive mode, use the **ip tcp intercept max-incomplete** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept max-incomplete **low** *number* **high** *number*

no ip tcp intercept max-incomplete [**low** *number* **high** *number*]

Syntax Description

low *number*	Defines the number of incomplete connections below which the software leaves aggressive mode. The range is 1 to 2147483647. The default is 900
high *number*	Defines the number of incomplete connections allowed, above which the software enters aggressive mode. The range is from 1 to 2147483647. The default is 1100.

Command Default

The number of incomplete connections below which the software leaves aggressive mode is 900.

The maximum number of incomplete connections allowed before the software enters aggressive mode is 1100.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)T	This command was introduced in Cisco IOS Release 12.4(15)T. This command replaces the **ip tcp intercept max-incomplete low** and the **ip tcp intercept max-incomplete high** commands.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

There are two factors that determine aggressive mode: connection requests and incomplete connections.

By default, if *both* the number of connection requests and the number of incomplete connections is 900 or lower, aggressive mode ends.

By default, if *either* the number of connection requests or the number of incomplete connections is 1100 or greater, aggressive mode begins.

The number of connection requests may be defined by the **ip tcp intercept one-minute** command and the number of incomplete connections may be defined by the **ip tcp intercept max-incomplete** command.

Characteristics of Aggressive Mode

The following are the characteristics of aggressive mode:

- Each new arriving connection causes the oldest partial connection to be deleted.

- The initial retransmission timeout, the total time the router attempts to establish the connection, is reduced from 1 second to 0.5 seconds.
- The watch-timeout period is reduced from 30 seconds to 15 seconds.

Examples

The following example sets the software to leave aggressive mode when the number of incomplete connections falls below 1000 and allows 1500 incomplete connections before the software enters aggressive mode. The running configuration is also shown.

```
Router(config)# ip tcp intercept max-incomplete low 1000 high 1500
Router(config)# show running config | i ip tcp

     ip tcp intercept one-minute low 1000 high 1400
```

Related Commands

Command	Description
ip tcp intercept drop-mode	Sets the TCP intercept drop mode.
ip tcp intercept one-minute	Defines the number of connection requests below which the software leaves aggressive mode and the number of connection requests received before the software enters aggressive mode.

ip tcp intercept max-incomplete high

Note Effective with Cisco IOS Release 12.2(33)SXH and Cisco IOS Release 12.4(15)T, the **ip tcp intercept max-incomplete high** command is replaced by the **ip tcp intercept max-incomplete** command. See the **ip tcp intercept max-incomplete** command for more information.

To define the maximum number of incomplete connections allowed before the software enters aggressive mode, use the **ip tcp intercept max-incomplete high** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept max-incomplete high *number*

no ip tcp intercept max-incomplete high [*number*]

Syntax Description

number	Defines the number of incomplete connections allowed, above which the software enters aggressive mode. The range is from 1 to 2147483647. The default is 1100.

Defaults

1100 incomplete connections

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.4(15)T	This command was replaced by the **ip tcp intercept max-incomplete** command.
12.2(33)SXH	This command was replaced by the **ip tcp intercept max-incomplete** command.

Usage Guidelines

Note If you are running Cisco IOS Release 12.2(33)SXH or Cisco IOS Release 12.4(15)T and issue the **ip tcp intercept max-incomplete high** command, it will be accepted by the router, but a message will be displayed stating that the **ip tcp intercept max-incomplete high** command has been replaced by the **ip tcp intercept max-incomplete** command.

If the number of incomplete connections exceeds the *number* configured, the TCP intercept feature becomes aggressive. The following are the characteristics of aggressive mode:

- Each new arriving connection causes the oldest partial connection to be deleted.

- The initial retransmission timeout is reduced by half to 0.5 seconds (and so the total time trying to establish the connection is cut in half).
- The watch-timeout is cut in half (from 30 seconds to 15 seconds).

You can change the drop strategy from the oldest connection to a random connection with the **ip tcp intercept drop-mode** command.

Note The two factors that determine aggressive mode (connection requests and incomplete connections) are related and work together. When the value of *either* **ip tcp intercept one-minute high** or **ip tcp intercept max-incomplete high** is exceeded, aggressive mode begins. When *both* connection requests and incomplete connections fall below the values of ip tcp intercept one-minute low and **ip tcp intercept max-incomplete low**, aggressive mode ends.

The software will back off from its aggressive mode when the number of incomplete connections falls below the number specified by the **ip tcp intercept max-incomplete low** command.

Examples

The following example allows 1500 incomplete connections before the software enters aggressive mode:

```
ip tcp intercept max-incomplete high 1500
```

Related Commands

Command	Description
ip tcp intercept drop-mode	Sets the TCP intercept drop mode.
ip tcp intercept max-incomplete low	Defines the number of incomplete connections below which the software leaves aggressive mode.
ip tcp intercept one-minute high	Defines the number of connection requests received in the last one-minutes sample period before the software enters aggressive mode.
ip tcp intercept one-minute low	Defines the number of connection requests below which the software leaves aggressive mode.

ip tcp intercept max-incomplete low

Note Effective with Cisco IOS Release 12.2(33)SXH and Cisco IOS Release 12.4(15)T, the **ip tcp intercept max-incomplete low** command is replaced by the **ip tcp intercept max-incomplete** command. See the **ip tcp intercept max-incomplete** command for more information.

To define the number of incomplete connections below which the software leaves aggressive mode, use the **ip tcp intercept max-incomplete low** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept max-incomplete low *number*

no ip tcp intercept max-incomplete low [*number*]

Syntax Description

number	Defines the number of incomplete connections below which the software leaves aggressive mode. The range is 1 to 2147483647. The default is 900.

Defaults

900 incomplete connections

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.4(15)T	This command was replaced by the **ip tcp intercept max-incomplete** command.
12.2(33)SXH	This command was replaced by the **ip tcp intercept max-incomplete** command.

Usage Guidelines

Note If you are running Cisco IOS Release 12.2(33)SXH, or Cisco IOS Release 12.4(15)T and issue the **ip tcp intercept max-incomplete low** command, it will be accepted by the router, but a message will be displayed stating that the **ip tcp intercept max-incomplete high** command has been replaced by the **ip tcp intercept max-incomplete** command.

When *both* connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low** and **ip tcp intercept max-incomplete low**, the TCP intercept feature leaves aggressive mode.

Note The two factors that determine aggressive mode (connection requests and incomplete connections) are related and work together. When the value of *either* **ip tcp intercept one-minute high** or **ip tcp intercept max-incomplete high** is exceeded, aggressive mode begins. When *both* connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low** and **ip tcp intercept max-incomplete low**, aggressive mode ends.

See the **ip tcp intercept max-incomplete high** command for a description of aggressive mode.

Examples

The following example sets the software to leave aggressive mode when the number of incomplete connections falls below 1000:

```
ip tcp intercept max-incomplete low 1000
```

Related Commands

Command	Description
ip tcp intercept drop-mode	Sets the TCP intercept drop mode.
ip tcp intercept max-incomplete high	Defines the maximum number of incomplete connections allowed before the software enters aggressive mode.
ip tcp intercept one-minute high	Defines the number of connection requests received in the last one-minutes sample period before the software enters aggressive mode.
ip tcp intercept one-minute low	Defines the number of connection requests below which the software leaves aggressive mode.

ip tcp intercept mode

To change the TCP intercept mode, use the **ip tcp intercept mode** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept mode {**intercept** | **watch**}

no ip tcp intercept mode [**intercept** | **watch**]

Syntax Description

intercept	Active mode in which the TCP intercept software intercepts TCP packets from clients to servers that match the configured access list and performs intercept duties. This is the default.
watch	Monitoring mode in which the software allows connection attempts to pass through the router and watches them until they are established.

Defaults

intercept

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When TCP intercept is enabled, it operates in intercept mode by default. In intercept mode, the software actively intercepts TCP SYN packets from clients to servers that match the specified access list. For each SYN, the software responds on behalf of the server with an ACK and SYN, and waits for an ACK of the SYN from the client. When that ACK is received, the original SYN is sent to the server, and the code then performs a three-way handshake with the server. Then the two half-connections are joined.

In watch mode, the software allows connection attempts to pass through the router, but watches them until they become established. If they fail to become established in 30 seconds (or the value set by the **ip tcp intercept watch-timeout** command), a Reset is sent to the server to clear its state.

Examples

The following example sets the mode to watch mode:

```
ip tcp intercept mode watch
```

Related Commands

Command	Description
ip tcp intercept watch-timeout	Defines how long the software will wait for a watched TCP intercept connection to reach established state before sending a reset to the server.

ip tcp intercept one-minute

To define both the number of connection requests below which the software leaves aggressive mode and the number of connection requests that can be received before the software enters aggressive mode, use the **ip tcp intercept one-minute** command in global configuration mode. To restore the default connection request settings, use the **no** form of this command.

ip tcp intercept one-minute low *number* **high** *number*

no ip tcp intercept one-minute [**low** *number* **high** *number*]

Syntax Description

low *number*	Specifies the number of connection requests in the last one-minute sample period below which the software leaves aggressive mode. The range is from 1 to 2147483647. The default is 900.
high *number*	Specifies the number of connection requests that can be received in the last one-minute sample period before the software enters aggressive mode. The range is 1 to 2147483647. The default is 1100.

Command Default

The default number of connection requests below which the software leaves aggressive mode is 900.

The default number of connection requests received before the software enters aggressive mode is 1100.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)T	This command was introduced in Cisco IOS Release 12.4(15)T. This command replaces the **ip tcp intercept one-minute low** and the **ip tcp intercept one-minute high** commands.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

There are two factors that determine aggressive mode: connection requests and incomplete connections.

By default, if *both* the number of connection requests and the number of incomplete connections is 900 or lower, aggressive mode ends.

By default, if *either* the number of connection requests or the number of incomplete connections is 1100 or greater, aggressive mode begins.

The number of connection requests may be defined by the **ip tcp intercept one-minute** command and the number of incomplete connections may be defined by the **ip tcp intercept max-incomplete** command. The default number of connection requests

Characteristics of Aggressive Mode

The following are the characteristics of aggressive mode:

- Each new arriving connection causes the oldest partial connection to be deleted.

- The initial retransmission timeout, the total time the router attempts to establish the connection, is reduced from 1 second to 0.5 seconds.
- The watch-timeout period is reduced from 30 seconds to 15 seconds.

Examples

The following example sets the software to leave aggressive mode when the number of connection requests falls below 1000 and allows 1400 connection requests before the software enters aggressive mode. The the running configuration is then shown.

```
Router(config)# ip tcp intercept one-minute low 1000 high 1400
Router(config)# show running configuration | i ip tcp

     ip tcp intercept one-minute low 1000 high 1400
```

Related Commands

Command	Description
ip tcp intercept drop-mode	Sets the TCP intercept drop mode.
ip tcp intercept max-incomplete	Defines the number of incomplete connections below which the software leaves aggressive mode or the maximum number of incomplete connections allowed before the software enters aggressive mode.

ip tcp intercept one-minute high

Note Effective with Cisco IOS Release 12.2(33)SXH and Cisco IOS Release 12.4(15)T the **ip tcp intercept one-minute high** command is replaced by the **ip tcp intercept one-minute** command. See the **ip tcp intercept one-minute** command for more information.

To define the number of connection requests received in the last one-minutes sample period before the software enters aggressive mode, use the **ip tcp intercept one-minute high** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept one-minute high *number*

no ip tcp intercept one-minute high [*number*]

Syntax Description

number	Specifies the number of connection requests that can be received in the last one-minute sample period before the software enters aggressive mode. The range is 1 to 2147483647. The default is 1100.

Defaults

1100 connection requests

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.4(15)T	This command was replaced by the **ip tcp intercept one-minute** command.
12.2(33)SXH	This command was replaced by the **ip tcp intercept one-minute** command.

Usage Guidelines

Note If you are running Cisco IOS Release 12.2(33)SXH or Cisco IOS Release 12.4(15)T and issue the **ip tcp intercept one-minute high** command, it will be accepted by the router, but a message will be displayed stating that the **ip tcp intercept one-minute high** command has been replaced by the **ip tcp intercept one-minute** command.

If the number of connection requests exceeds the *number* value configured, the TCP intercept feature becomes aggressive. The following are the characteristics of aggressive mode:

- Each new arriving connection causes the oldest partial connection to be deleted.
- The initial retransmission timeout is reduced by half to 0.5 seconds (and so the total time trying to establish the connection is cut in half).
- The watch-timeout is cut in half (from 30 seconds to 15 seconds).

You can change the drop strategy from the oldest connection to a random connection with the **ip tcp intercept drop-mode** command.

Note The two factors that determine aggressive mode (connection requests and incomplete connections) are related and work together. When the value of *either* **ip tcp intercept one-minute high** or **ip tcp intercept max-incomplete high** is exceeded, aggressive mode begins. When *both* connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low** and **ip tcp intercept max-incomplete low**, aggressive mode ends.

Examples

The following example allows 1400 connection requests before the software enters aggressive mode:

```
ip tcp intercept one-minute high 1400
```

Related Commands

Command	Description
ip tcp intercept drop-mode	Sets the TCP intercept drop mode.
ip tcp intercept max-incomplete high	Defines the maximum number of incomplete connections allowed before the software enters aggressive mode.
ip tcp intercept max-incomplete low	Defines the number of incomplete connections below which the software leaves aggressive mode.
ip tcp intercept one-minute low	Defines the number of connection requests below which the software leaves aggressive mode.

ip tcp intercept one-minute low

Note Effective with Cisco IOS Release 12.2(33)SXH and Cisco IOS Release 12.4(15)T, the **ip tcp intercept one-minute low** command is replaced by the **ip tcp intercept one-minute** command. See the **ip tcp intercept one-minute** command for more information.

To define the number of connection requests below which the software leaves aggressive mode, use the **ip tcp intercept one-minute low** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept one-minute low *number*

no ip tcp intercept one-minute low [*number*]

Syntax Description

number	Defines the number of connection requests in the last one-minute sample period below which the software leaves aggressive mode. The range is from 1 to 2147483647. The default is 900.

Defaults

900 connection requests

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.4(15)T	This command was replaced by the **ip tcp intercept one-minute** command.
12.2(33)SXH	This command was replaced by the **ip tcp intercept one-minute** command.

Usage Guidelines

Note If you are running Cisco IOS Release 12.2(33)SXH or Cisco IOS Release 12.4(15)T and issue the **ip tcp intercept one-minute low** command, it will be accepted by the router, but a message will be displayed stating that the **ip tcp intercept one-minute low** command has been replaced by the **ip tcp intercept one-minute** command.

When *both* connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low** and **ip tcp intercept max-incomplete low**, the TCP intercept feature leaves aggressive mode.

Note The two factors that determine aggressive mode (connection requests and incomplete connections) are related and work together. When the value of *either* **ip tcp intercept one-minute high** or **ip tcp intercept max-incomplete high** is exceeded, aggressive mode begins. When *both* connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low** and **ip tcp intercept max-incomplete low**, aggressive mode ends.

See the **ip tcp intercept one-minute high** command for a description of aggressive mode.

Examples

The following example sets the software to leave aggressive mode when the number of connection requests falls below 1000:

```
ip tcp intercept one-minute low 1000
```

Related Commands

Command	Description
ip tcp intercept drop-mode	Sets the TCP intercept drop mode.
ip tcp intercept max-incomplete high	Defines the maximum number of incomplete connections allowed before the software enters aggressive mode.
ip tcp intercept max-incomplete low	Defines the number of incomplete connections below which the software leaves aggressive mode.
ip tcp intercept one-minute high	Defines the number of connection requests received in the last one-minutes sample period before the software enters aggressive mode.

ip tcp intercept watch-timeout

To define how long the software will wait for a watched TCP intercept connection to reach established state before sending a reset to the server, use the **ip tcp intercept watch-timeout** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept watch-timeout *seconds*

no ip tcp intercept watch-timeout [*seconds*]

Syntax Description

seconds	Time (in seconds) that the software waits for a watched connection to reach established state before sending a Reset to the server. The minimum value is 1 second. The default is 30 seconds.

Defaults

30 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command if you have set the TCP intercept to passive watch mode and you want to change the default time the connection is watched. During aggressive mode, the watch timeout time is cut in half.

Examples

The following example sets the software to wait 60 seconds for a watched connection to reach established state before sending a Reset to the server:

```
ip tcp intercept watch-timeout 60
```

Related Commands

Command	Description
ip tcp intercept mode	Changes the TCP intercept mode.

ip traffic-export apply

To apply an IP traffic export profile or an IP traffic capture profile to a specific interface, use the **ip traffic-export apply** command in interface configuration mode. To remove an IP traffic export profile or an IP traffic capture profile from an interface, use the **no** form of this command.

ip traffic-export apply *profile-name*

no ip traffic-export apply *profile-name*

Cisco 1841, Cisco 2800 Series, and Cisco 3800 Series

ip traffic-export apply *profile-name* **size** *size*

no ip traffic-export apply *profile-name*

Syntax Description

profile-name	Name of the profile that is to be applied to a specified interface. The *profile-name* argument must match a name that was specified in the **ip traffic-export profile** command.
size	Optional. Used in IP traffic capture mode to set up a local capture buffer.
size	Optional. Specifies the size of the local capture buffer, in bytes.

Defaults

If you do not use this command, a sucessfully configured profile is not active.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.4(11)T	This command was updated to incorporate the **size** keyword and *size* argument for IP traffic capture mode on the Cisco 1841, Cisco 2800 series, and Cisco 3800 series routers.

Usage Guidelines

After you configure at least one export profile, use the **ip traffic-export apply** command to activate IP traffic export on the specified ingress interface.

After you configure a capture profile, use the **ip traffic-export apply** command to activate IP traffic capture on the specified ingress interface, and to specify the size of the local capture buffer.

Examples

The following example shows how to apply the export profile “corp1” to interface Fast Ethernet 0/0.

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list spam_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```

The following example shows how to apply the capture profile “corp2” to interface Fast Ethernet 0/0, and specify a capture buffer of 10,000,000 bytes.

```
Router(config)# ip traffic-export profile corp2 mode_capture
Router(config-rite)# bidirectional
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# length 512
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp2 size 10000000
```

After a profile is activated on the interface, a logging message such as the following will appear:

```
%RITE-5-ACTIVATE: Activated IP traffic export on interface FastEthernet 0/0.
```

After a profile is removed from the interface, a logging message such as the following will appear:

```
%RITE-5-DEACTIVATE: Deactivated IP traffic export on interface FastEthernet 0/0.
```

If you attempt to apply an incomplete profile to an interface, you will receive the following message:

```
Router(config-if)# ip traffic-export apply newone
RITE: profile newone has missing outgoing interface
```

Related Commands

Command	Description
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.
traffic-export	Controls the operation of IP traffic capture mode.

ip traffic-export profile

To create or edit an IP traffic export profile or an IP traffic capture profile and enable the profile on an ingress interface, use the **ip traffic-export profile** command in global configuration mode. To remove an IP traffic export profile from your router configuration, use the **no** form of this command.

ip traffic-export profile *profile-name*

no ip traffic-export profile *profile-name*

Cisco 1841, Cisco 2800 Series, and Cisco 3800 Series Routers

ip traffic-export profile *profile-name* **mode** {**capture** | **export**}

no ip traffic-export profile *profile-name*

Syntax Description

profile-name	IP traffic export profile name.
mode {**capture** | **export**}	Specifies either capture or export mode. • **capture**—Captures data to memory. • **export**—Exports data to an interface.

Defaults

A profile does not exist.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.4(11)T	This command was updated to incorporate the **mode**, **capture**, and **export** keywords on the Cisco 1841, Cisco 2800 series, and Cisco 3800 series routers.

Usage Guidelines

The **ip traffic-export profile** command allows you to begin a profile that can be configured to capture or export IP packets as they arrive on or leave from a selected router ingress interface.

When exporting IP packets, a designated egress interface exports IP packets out of the router. So, the router can export unaltered IP packets to a directly connected device.

When capturing IP packets, the packets are stored in local router memory. They may then be dumped to an external device.

IP Traffic Export Profiles

All exported IP traffic configurations are specified by profiles, which consist of RITE-related command-line interface (CLI) commands that control various attributes of both incoming and outgoing IP traffic. You can configure a router with multiple profiles. (Each profile must have a different name.) You can apply different profiles on different interfaces.

The two profiles to configure are:

- Global configuration profile, which you configure using the **ip traffic-export profile** command.
- Submode configuration profile, which you configure using any of the following RITE commands—**bidirectional**, **incoming**, **interface**, **mac-address**, and **outgoing**.

Use **interface** and **mac-address** commands to successfully create a profile. If you do not issue these commands, the user will receive a profile incomplete messages such as the following:

```
ip traffic-export profile newone
! No outgoing interface configured
! No destination mac-address configured
```

After you configure your profiles, you can apply the profiles to an interface with the **ip traffic-export apply profile** command, which will activate it.

IP Traffic Capture Profiles

On the Cisco 1841, Cisco 2800 series, and Cisco 3800 series routers, you can also configure IP traffic capture. A captured IP traffic configuration is specified by a profile, which consists of RITE-related command-line interface (CLI) commands that control various attributes of both incoming and outgoing IP traffic.

The two profiles that you should configure are:

- Global configuration profile, which you configure using the **ip traffic-export profile mode capture** command.
- Submode configuration profile, which you configure using any of the following RITE commands—**bidirectional**, **incoming**, **length**, and **outgoing**.

After you configure your profiles, you can apply the profiles to an interface with the **ip traffic-export apply profile** command, which will activate it.

When the IP traffic capture profile is applied to an interface, use the **traffic-export** command to control the capture of the traffic.

Note Cisco IOS Release 12.4(9)T and 12.4(15)T cannot capture outgoing router-generated Internet Control Message Protocol (ICMP) or IPsec traffic.

Examples

The following example shows how to configure the profile “corp1,” which sends captured IP traffic to host “00a.8aab.90a0” at the interface “FastEthernet 0/1.” This profile is also configured to export 1 in every 50 packets and to allow incoming traffic only from the access control list (ACL) “ham_ACL.”

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
```

```
Router(config-if)# ip traffic-export apply corp1
```

The following example shows how to configure the profile "corp2," which captures IP traffic and stores it in a local router memory buffer of 10,000,000 bytes. This profile also captures 1 in every 50 packets and allows incoming traffic only from the access control list (ACL) "ham_ACL."

```
Router(config)# ip traffic-export profile corp2 mode capture
Router(config-rite)# bidirectional
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# length 512
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp2 size 10000000
```

Related Commands

Command	Description
bidirectional	Enables incoming and outgoing IP traffic to be exported or captured across a monitored interface.
incoming	Configures filtering for incoming export or capture traffic.
interface (RITE)	Specifies the outgoing interface for exporting traffic
ip traffic-export apply profile	Applies an IP traffic export or IP traffic capture profile to a specific interface.
length	Specifies the length of the packet in capture mode.
mac-address	Specifies the Ethernet address of the destination host in traffic export.
outgoing	Configures filtering for outgoing export or capture traffic.
traffic-export interface	Controls the operation of IP traffic capture mode.

ip trigger-authentication (global)

To enable the automated part of double authentication at a device, use the **ip trigger-authentication** command in global configuration mode. To disable the automated part of double authentication, use the **no** form of this command.

ip trigger-authentication [**timeout** *seconds*] [**port** *number*]

no ip trigger-authentication

Syntax Description

timeout *seconds*	(Optional) Specifies how frequently the local device sends a User Datagram Protocol (UDP) packet to the remote host to request the user's username and password (or PIN). The default is 90 seconds. See "The Timeout Keyword" in the Usage Guidelines section for details.
port *number*	(Optional) Specifies the UDP port to which the local router should send the UPD packet requesting the user's username and password (or PIN). The default is port 7500. See "The Port Keyword" in the Usage Guidelines section for details.

Defaults

The default timeout is 90 seconds, and the default port number is 7500.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Configure this command on the local device (router or network access server) that remote users dial in to. Use this command only if the local device has already been configured to provide double authentication; this command enables automation of the second authentication of double authentication.

The timeout Keyword

During the second authentication stage of double authentication—when the remote user is authenticated—the remote user must send a username and password (or PIN) to the local device. With automated double authentication, the local device sends a UDP packet to the remote user's host during the second user-authentication stage. This UDP packet triggers the remote host to launch a dialog box requesting a username and password (or PIN).

If the local device does not receive a valid response to the UDP packet within a timeout period, the local device will send another UDP packet. The device will continue to send UDP packets at the timeout intervals until it receives a response and can authenticate the user.

By default, the UDP packet timeout interval is 90 seconds. Use the **timeout** keyword to specify a different interval.

(This timeout also applies to how long entries will remain in the remote host table; see the **show ip trigger-authentication** command for details.)

The port Keyword

As described in the previous section, the local device sends a UDP packet to the remote user's host to request the user's username and password (or PIN). This UDP packet is sent to UDP port 7500 by default. (The remote host client software listens to UDP port 7500 by default.) If you need to change the port number because port 7500 is used by another application, you should change the port number using the **port** keyword. If you change the port number you need to change it in both places—both on the local device and in the remote host client software.

Examples

The following example globally enables automated double authentication and sets the timeout to 120 seconds:

```
ip trigger-authentication timeout 120
```

Related Commands

Command	Description
ip trigger-authentication (interface)	Specifies automated double authentication at an interface.
show ip trigger-authentication	Displays the list of remote hosts for which automated double authentication has been attempted.

ip trigger-authentication (interface)

To specify automated double authentication at an interface, use the **ip trigger-authentication** command in interface configuration mode. To turn off automated double authentication at an interface, use the **no** form of this command.

ip trigger-authentication

no ip trigger-authentication

Syntax Description

This command has no arguments or keywords.

Defaults

Automated double authentication is not enabled for specific interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Configure this command on the local router or network access server that remote users dial into. Use this command only if the local device has already been configured to provide double authentication and if automated double authentication has been enabled with the **ip trigger-authentication** (global) command.

This command causes double authentication to occur automatically when users dial into the interface.

Examples

The following example turns on automated double authentication at the ISDN BRI interface BRI0:

```
interface BRI0
 ip trigger-authentication
 encapsulation ppp
 ppp authentication chap
```

Related Commands

Command	Description
ip trigger-authentication (global)	Enables the automated part of double authentication at a device.

ip urlfilter alert

To enable URL filtering system alert messages, use the **ip urlfilter alert** command in global configuration mode. To disable the system alert, use the **no** form of this command.

ip urlfilter alert [**vrf** *vrf-name*]

no ip urlfilter alert

Syntax Description

vrf *vrf-name*	(Optional) Enables URL filtering system alert messages only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

URL filtering messages are enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.

Usage Guidelines

Use the **ip urlfilter alert** command to display system messages, such as a server entering allow mode, a server going down, or a URL that is too long for the lookup request.

Examples

The following example shows how to enable URL filtering alert messages:

```
ip inspect name test http urlfilter
ip urlfilter cache 5
ip urlfilter exclusive-domain permit .weapons.com
ip urlfilter exclusive-domain deny .nbc.com
ip urlfilter exclusive-domain permit www.cisco.com
ip urlfilter audit-trail
ip urlfilter alert
ip urlfilter server vendor websense 192.168.3.1
```

Afterward, system alert messages such as the following are displayed:

```
%URLF-3-SERVER_DOWN:Connection to the URL filter server 10.92.0.9 is down
```

This level three LOG_ERR-type message is displayed when a configured URL filter server (UFS) goes down. When this happens, the firewall will mark the configured server as secondary and try to bring up one of the other secondary servers and mark that server as the primary server. If there is no other server configured, the firewall will enter into allow mode and display the URLF-3-ALLOW_MODE message described.

```
%URLF-3-ALLOW_MODE:Connection to all URL filter servers are down and ALLOW MODE is OFF
```

This LOG_ERR type message is displayed when all UFSs are down and the system enters into allow mode.

Note Whenever the system goes into allow mode (all filter servers are down), a periodic keepalive timer will be triggered that will try to bring up a server by opening a TCP connection.

```
%URLF-5-SERVER_UP:Connection to an URL filter server 10.92.0.9 is made, the system is
returning from ALLOW MODE
```

This LOG_NOTICE-type message is displayed when the UFSs are detected as being up and the system is returning from allow mode.

```
%URLF-4-URL_TOO_LONG:URL too long (more than 3072 bytes), possibly a fake packet?
```

This LOG_WARNING-type message is displayed when the URL in a lookup request is too long; any URL longer than 3K will be dropped.

```
%URLF-4-MAX_REQ:The number of pending request exceeds the maximum limit <1000>
```

This LOG_WARNING-type message is displayed when the number of pending requests in the system exceeds the maximum limit and all further requests are dropped.

ip urlfilter allowmode

To turn on the default mode (allow mode) of the filtering algorithm, use the **ip urlfilter allowmode** command in global configuration mode. To disable the default mode, use the **no** form of this command.

ip urlfilter allowmode [**on** | **off**] [**vrf** *vrf-name*]

no ip urlfilter allowmode [**on** | **off**]

Syntax Description

on	(Optional) Allow mode is on.
off	(Optional) Allow mode is off.
vrf *vrf-name*	(Optional) Turns on the default mode of the filtering algorithm only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

Allow mode is off.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.

Usage Guidelines

The system will go into allow mode when connections to all vendor servers (Websense or N2H2) are down. The system will return to normal mode when a connection to at least one web vendor server is up. Allow mode directs your system to forward or drop all packets on the basis of the configurable allow mode setting: if allow mode is on and the vendor servers are down, the HTTP requests will be allowed to pass; if allow mode is off and the vendor servers are down, the HTTP requests will be forbidden.

Examples

The following example shows how to enable allow mode on your system:

```
ip urlfilter allowmode on
```

Afterward, the following alert message will be displayed when the system goes into allow mode:

```
%URLF-3-ALLOW_MODE: Connection to all URL filter servers are down and ALLOW MODE if OFF
```

The following alert message will be displayed when the system returns from allow mode:

```
%URLF-5-SERVER_UP: Connection to an URL filter server 12.0.0.3 is made, the system is
returning from allow mode
```

ip urlfilter audit-trail

To log messages into the syslog server or router, use the **ip urlfilter audit-trail** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip urlfilter audit-trail [**vrf** *vrf-name*]

no ip urlfilter audit-trail

Syntax Description

vrf *vrf-name*	(Optional) Logs messages into the syslog server or router only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.

Usage Guidelines

Use the **ip urlfilter audit-trail** command to log messages such as URL request status (allow or deny) into your syslog server.

Examples

The following example shows how to enable syslog message logging:

```
ip inspect name test http urlfilter
ip urlfilter cache 5
ip urlfilter exclusive-domain permit .weapons.com
ip urlfilter exclusive-domain deny .nbc.com
ip urlfilter exclusive-domain permit www.cisco.com
ip urlfilter audit-trail
ip urlfilter alert
ip urlfilter server vendor websense 209.165.202.130
```

Afterward, audit trail messages such as the following are displayed and logged into the log server:

```
%URLF-6-SITE_ALLOWED:Client 209.165.201.15:12543 accessed server 10.76.82.21:8080
```

This message is logged for each request whose destination IP address is found in the cache. It includes the source IP address, source port number, destination IP address, and destination port number. The URL is not logged in this case because the IP address of the request is found in the cache; thus, parsing the request and extracting the URL is a waste of time.

```
%URLF-4-SITE-BLOCKED: Access denied for the site 'www.sports.com'; client
209.165.200.230:34557 server 209.165.201.2:80
```

This message is logged when a request finds a match against one of the blocked domains in the exclusive-domain list or the corresponding entry in the IP cache.

```
%URLF-6-URL_ALLOWED:Access allowed for URL http://www.N2H2.com/; client
209.165.200.230:54123  server 192.168.0.1:80
```

This message is logged for each URL request that is allowed by the vendor server (Websense or N2H2). It includes the allowed URL, source IP address, source port number, destination IP address, and destination port number. Longer URLs will be truncated to 300 bytes and then logged.

```
%URLF-6-URL_BLOCKED:Access denied URL http://www.google.com; client 209.165.200.230:54678
server 209.165.201.2:80
```

This message is logged for each URL request that is blocked by the vendor server. It includes the blocked URL, source IP address, source port number, destination IP address, and destination port number. Longer URLs will be truncated to 300 bytes and then logged.

ip urlfilter cache

To configure cache parameters, use the **ip urlfilter cache** command in global configuration mode. To clear the configuration, use the **no** form of this command.

ip urlfilter cache number [**vrf** *vrf-name*]

no ip urlfilter cache number

Syntax Description

number	Maximum number of destination IP addresses that can be cached into the cache table. The default value is 5000.
vrf *vrf-name*	(Optional) Configures cache parameters only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

Maximum number of destination IP addresses is 5000.

The cache table is cleared out every 12 hours.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.

Usage Guidelines

The cache table consists of the most recently requested IP addresses and respective authorization status for each IP address.

The caching algorithm involves three parameters—the maximum number of IP addresses that can be cached, an idle time, and an absolute time. The algorithm also involves two timers—idle timer and absolute timer. The idle timer is a small periodic timer (1 minute) that checks to see whether the number of cached IP addresses in the cache table exceeds 80 percent of the maximum limit. If the cached IP addresses have exceeded 80 percent, it will start removing idle entries; if it has not exceeded 80 percent, it will quit and wait for the next cycle. The absolute timer is a large periodic timer (1 hour) that is used to remove all of the elapsed entries. (The age of an elapsed entry is greater than the absolute time.) An elapsed entry will also be removed during cache lookup.

The idle time value is fixed at 10 minutes. The absolute time value is taken from the vendor server look-up response, which is often greater than 15 hours. The absolute value for cache entries made out of exclusive-domains is 12 hours. The maximum number of cache entries is configurable by enabling the **ip urlfilter cache** command.

Note The vendor server is not able to inform the Cisco IOS firewall of filtering policy changes in the database.

Examples

The following example shows how to configure the cache table to hold a maximum of five destination IP addresses:

```
ip inspect name test http urlfilter
ip urlfilter cache 5
ip urlfilter exclusive-domain permit .weapons.com
ip urlfilter exclusive-domain deny .nbc.com
ip urlfilter exclusive-domain permit www.cisco.com
ip urlfilter audit-trail
ip urlfilter alert
ip urlfilter server vendor websense 192.168.3.1
```

Related Commands

Command	Description
clear ip urlfilter cache	Clears the cache table.
show ip urlfilter cache	Displays the destination IP addresses that are cached into the cache table.

ip urlfilter exclusive-domain

To add or remove a domain name to or from the exclusive domain list so that the firewall does not have to send lookup requests to the vendor server, use the **ip urlfilter exclusive-domain** command in global configuration mode. To remove a domain name from the exclusive domain name list, use the **no** form of this command.

ip urlfilter exclusive-domain {**permit** | **deny**} *domain-name* [**vrf** *vrf-name*]

no ip urlfilter exclusive-domain {**permit** | **deny**} *domain-name*

Syntax Description

permit	Permits all traffic destined for the specified domain name.
deny	Blocks all traffic destined for the specified domain name.
domain-name	Domain name that is added or removed from the exclusive domain name list; for example, www.cisco.com.
vrf *vrf-name*	(Optional) Adds or removes a domain name only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

This command is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.

Usage Guidelines

The **ip urlfilter exclusive-domain** command allows you to specify a list of domain names (exclusive domains) so that the firewall will not create a lookup request for the HTTP traffic that is destined for one of the domains in the exclusive list. Thus, you can avoid sending look-up requests to the web server for HTTP traffic that is destined for a host that is completely allowed to all users.

Flexibility when entering domain names is also provided; that is, the user can enter the complete domain name or a partial domain name.

Complete Domain Name

If the user adds a complete domain name, such as “www.cisco.com,” to the exclusive domain list, all HTTP traffic whose URLs are destined for this domain (such as www.cisco.com/news and www.cisco.com/index) will be excluded from the URL filtering policies of the vendor server (Websense or N2H2), and on the basis of the configuration, the URLs will be permitted or blocked (denied).

Partial Domain Name

If the user adds only a partial domain name to the exclusive domain list, such as ".cisco.com," all URLs whose domain names end with this partial domain name (such as www.cisco.com/products and www.cisco.com/eng) will be excluded from the URL filtering policies of the vendor server (Websense or N2H2), and on the basis of the configuration, the URLs will be permitted or blocked (denied).

Examples

The following example shows how to add the complete domain name "www.cisco.com" to the exclusive domain name list. This configuration will block all traffic destined to the www.cisco.com domain.

```
ip urlfilter exclusive-domain deny www.cisco.com
```

The following example shows how to add the partial domain name ".cisco.com" to the exclusive domain name list. This configuration will permit all traffic destined to domains that end with .cisco.com.

```
ip urlfilter exclusive-domain permit .cisco.com
```

ip urlfilter max-request

To set the maximum number of outstanding requests that can exist at any given time, use the **ip urlfilter max-request** command in global configuration mode. To disable this function, use the **no** form of this command.

ip urlfilter max-request *number* [**vrf** *vrf-name*]

no ip urlfilter max-request *number*

Syntax Description

number	Maximum number of outstanding requests. The default value is 1000.
vrf *vrf-name*	(Optional) Sets the maximum number of outstanding requests only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

Maximum number of requests is 1000.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.

Usage Guidelines

If the specified maximum number of outstanding requests is exceeded, new requests will be dropped.

Note Allow mode is not considered because it should be used only when servers are down.

Examples

The following example shows how to configure the maximum number of outstanding requests to 950:

```
ip inspect name url_filter http
ip urlfilter max-request 950
```

Related Commands

Command	Description
ip inspect name	Defines a set of inspection rules.
ip urlfilter server vendor	Configures a vendor server for URL filtering.

ip urlfilter max-resp-pak

To configure the maximum number of HTTP responses that the firewall can keep in its packet buffer, use the **ip urlfilter max-resp-pak** command in global configuration mode. To return to the default, use the **no** form of this command.

ip urlfilter max-resp-pak *number* [**vrf** *vrf-name*]

no ip urlfilter max-resp-pak *number*

Syntax Description

number	Maximum number of HTTP responses that can be stored in the packet buffer of the firewall. After the maximum number has been reached, the firewall will drop further responses. The default, and absolute maximum, value is 200.
vrf *vrf-name*	(Optional) Sets the maximum number of HTTP responses only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

200 HTTP responses

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.

Usage Guidelines

When an HTTP request arrives at a Cisco IOS firewall, the firewall forwards the request to the web server while simultaneously sending a URL look-up request to the vendor server (Websense or N2H2). If the vendor server reply arrives before the HTTP response, the firewall will know whether to permit or block the HTTP response; if the HTTP response arrives before the vendor server reply, the firewall will not know whether to allow or block the response, so the firewall will drop the response until it hears from the vendor server. The **ip urlfilter max-resp-pak** command allows you to configure your firewall to store the HTTP responses in a buffer, which allows your firewall to store a maximum of 200 HTTP responses. Each response will remain in the buffer until an allow or deny message is received from the vendor server. If the vendor server reply allows the URL, the firewall will release the HTTP response from the buffer to the end user; if the vendor server reply denies the URL, the firewall will discard the HTTP response from the buffer and close the connection to both ends.

Examples

The following example shows how to configure your firewall to hold 150 HTTP responses:

```
ip urlfilter max-resp-pak 150
```

ip urlfilter server vendor

To configure a vendor server for URL filtering, use the **ip urlfilter server vendor** command in global configuration mode. To remove a server from your configuration, use the **no** form of this command.

ip urlfilter server vendor {**websense** | **n2h2**} *ip-address* [**port** *port-number*] [**timeout** *seconds*] [**retransmit** *number*] [**outside**] [**vrf** *vrf-name*]

no ip urlfilter server vendor {**websense** | **n2h2**} *ip-address* [**port** *port-number*] [**timeout** *seconds*] [**retransmit** *number*] [**outside**]

Syntax Description

websense	Websense server will be used.
n2h2	N2H2 server will be used.
ip-address	IP address of the vendor server.
port *port-number*	(Optional) Port number that the vendor server listens on. The default port number is 15868.
timeout *seconds*	(Optional) Length of time, in seconds, that the Cisco IOS firewall will wait for a response from the vendor server. The default timeout is 5 seconds.
retransmit *number*	(Optional) Number of times the Cisco IOS firewall will retransmit the request when a response does not arrive for the request. The default value is two times.
outside	(Optional) Vendor server will be deployed on the outside network.
vrf *vrf-name*	(Optional) Configures a vendor server for URL filtering only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

A vendor server is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(2)T	The **outside** keyword was added.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.

Usage Guidelines

Use the **ip urlfilter server vendor** command to configure a Websense or N2H2 server, which will interact with the Cisco IOS Firewall to filter HTTP requests on the basis of a specified policy—global filtering, user- or group-based filtering, keyword-based filtering, category-based filtering, or customized filtering.

If the firewall has not received a response from the vendor server within the time specified in the **timeout** *seconds* keyword and argument, the firewall will check the **retransmit** *number* keyword and argument configured for the vendor server. If the firewall *has not* exceeded the maximum retransmit tries allowed, it will resend the HTTP lookup request. If the firewall *has* exceeded the maximum retransmit tries allowed, it will delete the outstanding request from the queue and check the status of the allow mode value. The firewall will forward the request if the allow mode is on; otherwise, it will drop the request.

By default, URL lookup requests that are made to the vendor server contain non-natted client IP addresses because the vendor server is deployed on the inside network. The **outside** keyword allows the vendor server to be deployed on the outside network, thereby, allowing Cisco IOS software to send the natted IP address of the client in the URL lookup request.

Primary and Secondary Servers

When users configure multiple vendor servers, the firewall will use only one server at a time—the primary server; all other servers are called secondary servers. When the primary server becomes unavailable for any reason, it becomes a secondary server and one of the secondary servers becomes the primary server.

A firewall marks a primary server as down when sending a request to or receiving a response from the server fails. When a primary server goes down, the system will go to the beginning of the configured servers list and try to activate the first server on the list. If the first server on the list is unavailable, it will try the second server on the list; the system will keep trying to activate a server until it is successful or until it reaches the end of the server list. If the system reaches the end of the server list, it will set a flag indicating that all of the servers are down, and it will enter allow mode.

Examples

The following example shows how to configure the Websense server for URL filtering:

```
ip inspect name test http urlfilter
ip urlfilter cache 5
ip urlfilter exclusive-domain permit .weapons.com
ip urlfilter exclusive-domain deny .nbc.com
ip urlfilter exclusive-domain permit www.cisco.com
ip urlfilter audit-trail
ip urlfilter alert
ip urlfilter server vendor websense 192.168.3.1
```

Related Commands

Command	Description
ip urlfilter allowmode	Turns on the default mode (allow mode) of the filtering algorithm.
ip urlfilter max-request	Sets the maximum number of outstanding requests that can exist at any given time.

ip urlfilter source-interface

To allow the URL filter to specify the interface whose IP address is used as the source IP address while a TCP connection is made to the URL filter server (Websense or N2H2), use the **ip urlfilter source-interface** command in global configuration mode. To disable the option, use the **no** form of this command.

ip urlfilter source-interface *interface-type* [**vrf** *vrf-name*]

no ip urlfilter source-interface [**vrf** *vrf-name*]

Syntax Description

interface-type	The interface type that is used as the source IP address.
vrf *vrf-name*	(Optional) Specifies the Virtual Routing and Forwarding (VRF) interface.

Command Default

The URL filter to specify a source interface for TCP is not defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The **ip urlfilter source-interface** command is used to define the source interface from which the URL filter request is sent. This command is recommended to be configured if the URL filter server can only be routed through certain interfaces on the router.

Examples

The following example shows that the URL filtering server is routed to the Ethernet interface type:

```
Router(config)# ip urlfilter source-interface ethernet
```

Related Commands

Command	Description
debug ip urlfilter	Enables debug information of URL filter subsystems.

ip urlfilter truncate

To allow the URL filter to truncate long URLs to the server, use the **ip urlfilter truncate** command in global configuration mode. To disable the truncating option, use the **no** form of this command.

ip urlfilter truncate {**script-parameters** | **hostname**} [**vrf** *vrf-name*]

no ip urlfilter truncate {**script-parameters** | **hostname**} [**vrf** *vrf-name*]

Syntax Description

script-parameters	Specifies that only the URL up to the script options is sent. • For example, if the entire URL is http://www.cisco.com/dev/xxx.cgi?when=now, only the URL through http://www.cisco.com/dev/xxx.cgi is sent (if the maximum supported URL length is not exceeded).
hostname	Specifies that only the hostname is sent. • For example, if the entire URL is http://www.cisco.com/dev/xxx.cgi?when=now, only http://www.cisco.com is sent.
vrf *vrf-name*	(Optional) Specifies the Virtual Routing and Forwarding (VRF) interface.

Command Default

URLs that are longer than the maximum supported length are not truncated, and the HTTP request is rejected.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

If both the **script-parameters** and **hostname** keywords are configured, the **script-parameters** keyword takes precedence over the **hostname** keyword. If both the keywords are configured and the script parameters URL is truncated and the maximum supported URL length is exceeded, the URL is truncated up to the hostname.

Note If both **script-parameters** and **hostname** keywords are configured, they must be on separate lines as shown in the "Examples" section. They cannot be combined in one line.

Examples

The following example shows that the URL is to be truncated up to the script options:

```
ip urlfilter truncate script-parameters
```

The following example shows that the URL is to be truncated up to the hostname:

```
ip urlfilter truncate hostname
```

Related Commands

Command	Description
debug ip urlfilter	Enables debug information of URL filter subsystems.

ip urlfilter urlf-server-log

To enable the logging of system messages on the URL filtering server, use the **ip urlfilter urlf-server-log** command in global configuration mode. To disable the logging of system messages, use the **no** form of this command.

ip urlfilter urlf-server-log [**vrf** *vrf-name*]

no ip urlfilter urlf-server-log

Syntax Description

vrf *vrf-name*	(Optional) Enables the logging of system messages on the URL filtering server only for the specified Virtual Routing and Forwarding (VRF) interface.

Defaults

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.

Usage Guidelines

Use the **ip urlfilter urlf-server-log** command to enable Cisco IOS to send a log request immediately after the URL lookup request. The firewall will not make a URL lookup request if the destination IP address is in the cache, but it will still make a log request to the server. (The log request contains the URL, hostname, source IP address, and the destination IP address.) The server records the log request into its own log server so your can view this information as necessary.

Examples

The following example shows how to enable system message logging on the URL filter server:

```
ip urlfilter urlf-server-log
```

ip verify drop-rate compute interval

To configure the interval of time between Unicast Reverse Path Forwarding (RPF) drop rate computations, use the **ip verify drop-rate compute interval** command in global configuration mode. To reset the interval to the default value, use the **no** form of this command.

ip verify drop-rate compute interval *seconds*

no ip verify drop-rate compute interval

Syntax Description

seconds	Interval, in seconds, between Unicast RPF drop rate computations. The range is from 30 to 300. The default is 30.

Command Default

The drop rate is not computed.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI2	This command was integrated into Cisco IOS Release 12.2(33)SXI2.

Usage Guidelines

The configured value applies for the computation of all Unicast RPF drop rates (global and per interface).

The value for the compute interval must be less than or equal to the value configured using the **ip verify drop-rate compute window** command. If you configure the **no** form of the **ip verify drop-rate compute interval** command while the cipUrpfDropRateWindow value is configured to be less than the default compute interval value, the following message appears on the console:

```
"urpf drop rate window < interval"
```

This error message means the command was not executed. The compute interval remains at the configured value rather than changing to the default value.

Examples

The following example shows how to configure a compute interval of 45 seconds:

```
Router> enable
Router# configure terminal
Router(config)# ip verify drop-rate compute interval 45
```

Related Commands

Command	Description
ip verify drop-rate compute window	Configures the interval of time during which the Unicast RPF drop count is collected for the drop rate computation.
ip verify drop-rate notify hold-down	Configures the minimum time between Unicast RPF drop rate notifications.
ip verify unicast notification threshold	Configures the threshold value used to determine whether to send a Unicast RPF drop rate notification.

ip verify drop-rate compute window

To configure the interval of time during which the Unicast Reverse Path Forwarding (RPF) drop count is collected for the drop rate computation, use the **ip verify drop-rate compute window** command in global configuration mode. To reset the window to the default value, use the **no** form of this command.

ip verify drop-rate compute window *seconds*

no ip verify drop-rate compute window

Syntax Description

seconds	Interval, in seconds, during which the Unicast RPF drop count is accumulated for the drop rate computation. The range is from 30 to 300. The default is 300.

Command Default

The drop rate is not calculated.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI2	This command was integrated into Cisco IOS Release 12.2(33)SXI2.

Usage Guidelines

This command configures the sliding window that begins the configured number of seconds prior to the computation and ends with the Unicast RPF drop rate computation. The configured value applies for the computation of all Unicast RPF drop rates (global and per interface).

The value configured for the “compute window” must be greater than or equal to the value configured using the **ip verify drop-rate compute interval** command. If you configure the **no** form of the **ip verify drop-rate compute window** command while the cipUrpfDropRateInterval value is configured to be greater than the default compute window value, the following message appears on the console:

```
“urpf drop rate window < interval”
```

This error message means that the command was not executed. The compute window remains at the configured value rather than changing to the default value.

Examples

The following example shows how to configure a compute window of 60 seconds:

```
Router> enable
Router# configure terminal
Router(config)# ip verify drop-rate compute window 60
```

Related Commands

Command	Description
ip verify drop-rate compute interval	Configures the interval between Unicast RPF drop rate computations.
ip verify drop-rate notify hold-down	Configures the minimum time between Unicast RPF drop rate notifications.
ip verify unicast notification threshold	Configures the threshold value used to determine whether to send a Unicast RPF drop rate notification.

ip verify drop-rate notify hold-down

To configure the minimum time between Unicast Reverse Path Forwarding (RPF) drop rate notifications, use the **ip verify drop-rate notify hold-down** command in global configuration mode. To reset the hold-down time to the default value, use the **no** form of this command.

ip verify drop-rate notify hold-down *seconds*

no ip verify drop-rate notify hold-down

Syntax Description

seconds	Minimum time, in seconds, between Unicast RPF drop rate notifications. The range is from 30 to 300. The default is 300.

Command Default

No notifications are sent.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI2	This command was integrated into Cisco IOS Release 12.2(33)SXI2.

Usage Guidelines

The configured value applies for the computation of all Unicast RPF drop rates (global and per interface).

Examples

The following example shows how to configure a notify hold-down time of 40 seconds:

```
Router> enable
Router# configure terminal
Router(config)# ip verify drop-rate notify hold-down 40
```

Related Commands

Command	Description
ip verify drop-rate compute interval	Configures the interval of time between Unicast RPF drop rate computations.
ip verify drop-rate compute window	Configures the interval of time over which the Unicast RPF drop count used in the drop rate computation is collected.
ip verify unicast notification threshold	Configures the threshold value used to determine whether to send a Unicast RPF drop rate notification.

ip verify unicast notification threshold

To configure the threshold value used to determine whether to send a Unicast Reverse Path Forwarding (RPF) drop rate notification, use the **ip verify unicast notification threshold** command in interface configuration mode. To set the notification threshold back to the default value, use the **no** form of this command.

ip verify unicast notification threshold *rate-val*

no ip verify unicast notification threshold

Syntax Description

rate-val	Threshold value, in packets per second, used to determine whether to send a Unicast RPF drop rate notification. The range is from 0 to 4294967295. The default is 1000.

Command Default

No notifications are sent.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI2	This command was integrated into Cisco IOS Release 12.2(33)SXI2.

Usage Guidelines

This command configures the threshold Unicast RPF drop rate which, when exceeded, triggers a notification. Configuring a value of 0 means that any Unicast RPF packet drop triggers a notification.

Examples

The following example shows how to configure a notification threshold value of 900 on Ethernet interface 3/0:

```
Router> enable
Router# configure terminal
Router(config# interface ethernet 3/0
Router(config-if)# ip verify unicast notification threshold 900
```

Related Commands

Command	Description
ip verify drop-rate compute interval	Configures the interval of time between Unicast RPF drop rate computations.
ip verify drop-rate compute window	Configures the interval of time during which the Unicast RPF drop count is collected for the drop rate computation.
ip verify drop-rate notify hold-down	Configures the minimum time between Unicast RPF drop rate notifications.

ip verify unicast reverse-path

Note This command was replaced by the **ip verify unicast source reachable-via** command effective with Cisco IOS Release 12.0(15)S. The **ip verify unicast source reachable-via** command allows for more flexibility and functionality, such as supporting asymmetric routing, and should be used for any Reverse Path Forward implementation. The **ip verify unicast reverse-path** command is still supported.

To enable Unicast Reverse Path Forwarding (Unicast RPF), use the **ip verify unicast reverse-path** command in interface configuration mode. To disable Unicast RPF, use the **no** form of this command.

ip verify unicast reverse-path [*list*]

no ip verify unicast reverse-path [*list*]

Syntax Description

list	(Optional) Specifies a numbered access control list (ACL) in the following ranges: • 1 to 99 (IP standard access list) • 100 to 199 (IP extended access list) • 1300 to 1999 (IP standard access list, expanded range) • 2000 to 2699 (IP extended access list, expanded range)

Command Default

Unicast RPF is disabled.

Command Modes

Interface configuration mode (config-if)

CommandHistory

Release	Modification
11.1(CC), 12.0	This command was introduced. This command was not included in Cisco IOS Release 11.2 or 11.3
12.1(2)T	Added ACL support using the *list* argument. Added per-interface statistics on dropped or suppressed packets.
12.0(15)S	The **ip verify unicast source reachable-via** command replaced this command, and the following keywords were added to the **ip verify unicast source reachable-via** command: **allow-default, allow-self-ping**, **rx**, and **any**.
12.1(8a)E	The **ip verify unicast reverse-path** command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(14)S	The **ip verify unicast reverse-path** command was integrated into Cisco IOS Release 12.2(14)S.

Release	Modification
12.2(14)SX	The **ip verify unicast reverse-path** command was integrated into Cisco IOS Release 12.2(14)SX.
12.2(33)SRA	The **ip verify unicast reverse-path** command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **ip verify unicast reverse-path interface** command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that are received by a router. Malformed or forged source addresses can indicate denial of service (DoS) attacks on the basis of source IP address spoofing.

When Unicast RPF is enabled on an interface, the router examines all packets that are received on that interface. The router checks to ensure that the source address appears in the Forwarding Information Base (FIB) and that it matches the interface on which the packet was received. This "look backwards" ability is available only when Cisco Express Forwarding (CEF) is enabled on the router because the lookup relies on the presence of the FIB. CEF generates the FIB as part of its operation.

To use Unicast RPF, enable CEF switching or distributed CEF (dCEF) switching in the router. There is no need to configure the input interface for CEF switching. As long as CEF is running on the router, individual interfaces can be configured with other switching modes.

Note It is very important for CEF to be configured globally in the router. Unicast RPF will not work without CEF.

Note Unicast RPF is an input function and is applied on the interface of a router only in the ingress direction.

The Unicast Reverse Path Forwarding feature checks to determine whether any packet that is received at a router interface arrives on one of the best return paths to the source of the packet. The feature does this by doing a reverse lookup in the CEF table. If Unicast RPF does not find a reverse path for the packet, Unicast RPF can drop or forward the packet, depending on whether an ACL is specified in the Unicast Reverse Path Forwarding command. If an ACL is specified in the command, then when (and only when) a packet fails the Unicast RPF check, the ACL is checked to determine whether the packet should be dropped (using a deny statement in the ACL) or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for Unicast RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the Unicast Reverse Path Forwarding command, the router drops the forged or malformed packet immediately and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

Unicast RPF events can be logged by specifying the logging option for the ACL entries used by the Unicast Reverse Path Forwarding command. Log information can be used to gather information about the attack, such as source address, time, and so on.

Where to Use RPF in Your Network

Unicast RPF may be used on interfaces in which only one path allows packets from valid source networks (networks contained in the FIB). Unicast RPF may also be used in cases for which a router has multiple paths to a given network, as long as the valid networks are switched via the incoming interfaces. Packets for invalid networks will be dropped. For example, routers at the edge of the network of an

Internet Service Provider (ISP) are likely to have symmetrical reverse paths. Unicast RPF may still be applicable in certain multi-homed situations, provided that optional Border Gateway Protocol (BGP) attributes such as weight and local preference are used to achieve symmetric routing.

With Unicast RPF, all equal-cost "best" return paths are considered valid. This means that Unicast RPF works in cases where multiple return paths exist, provided that each path is equal to the others in terms of the routing cost (number of hops, weights, and so on) and as long as the route is in the FIB. Unicast RPF also functions where Enhanced Internet Gateway Routing Protocol (EIGRP) variants are being used and unequal candidate paths back to the source IP address exist.

For example, routers at the edge of the network of an ISP are more likely to have symmetrical reverse paths than routers that are in the core of the ISP network. Routers that are in the core of the ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router. In this scenario, you should use the new form of the command, **ip verify unicast source reachable-via**, if there is a chance of asymmetrical routing.

Examples

The following example shows that the Unicast Reverse Path Forwarding feature has been enabled on a serial interface:

```
ip cef
! or "ip cef distributed" for RSP+VIP based routers
!
interface serial 5/0/0
 ip verify unicast reverse-path
```

The following example uses a very simple single-homed ISP to demonstrate the concepts of ingress and egress filters used in conjunction with Unicast RPF. The example illustrates an ISP-allocated classless interdomain routing (CIDR) block 192.168.202.128/28 that has both inbound and outbound filters on the upstream interface. Be aware that ISPs are usually not single-homed. Hence, provisions for asymmetrical flows (when outbound traffic goes out one link and returns via a different link) need to be designed into the filters on the border routers of the ISP.

```
ip cef distributed
!
interface Serial 5/0/0
 description Connection to Upstream ISP
 ip address 192.168.200.225 255.255.255.255
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp
 ip verify unicast reverse-path
 ip access-group 111 in
 ip access-group 110 out
!
access-list 110 permit ip 192.168.202.128 10.0.0.31 any
access-list 110 deny ip any any log
access-list 111 deny ip host 10.0.0.0 any log
access-list 111 deny ip 172.16.0.0 255.255.255.255 any log
access-list 111 deny ip 10.0.0.0 255.255.255.255 any log
access-list 111 deny ip 172.16.0.0 255.255.255.255 any log
access-list 111 deny ip 192.168.0.0 255.255.255.255 any log
access-list 111 deny ip 209.165.202.129 10.0.0.31 any log
access-list 111 permit ip any any
```

The following example demonstrates the use of ACLs and logging with Unicast RPF. In this example, extended ACL 197 provides entries that deny or permit network traffic for specific address ranges. Unicast RPF is configured on interface Ethernet 0 to check packets arriving at that interface.

For example, packets with a source address of 192.168.201.10 arriving at interface Ethernet 0 are dropped because of the deny statement in ACL 197. In this case, the ACL information is logged (the logging option is turned on for the ACL entry) and dropped packets are counted per-interface and globally. Packets with a source address of 192.168.201.100 arriving at interface Ethernet 0 are forwarded because of the permit statement in ACL 197. ACL information about dropped or suppressed packets is logged (the logging option is turned on for the ACL entry) to the log server.

```
ip cef distributed
!
int eth0/1/1
 ip address 192.168.200.1 255.255.255.255
 ip verify unicast reverse-path 197
!
int eth0/1/2
 ip address 192.168.201.1 255.255.255.255
!
access-list 197 deny   ip 192.168.201.0 10.0.0.63 any log-input
access-list 197 permit ip 192.168.201.64 10.0.0.63 any log-input
access-list 197 deny   ip 192.168.201.128 10.0.0.63 any log-input
access-list 197 permit ip 192.168.201.192 10.0.0.63 any log-input
access-list 197 deny ip host 10.0.0.0 any log-input
access-list 197 deny ip 172.16.0.0 255.255.255.255 any log-input
access-list 197 deny ip 10.0.0.0 255.255.255.255 any log-input
access-list 197 deny ip 172.16.0.0 255.255.255.255 any log-input
access-list 197 deny ip 192.168.0.0 255.255.255.255 any log-input
```

Related Commands

Command	Description
ip cef	Enables CEF on the route processor card.

ip verify unicast source reachable-via

To enable Unicast Reverse Path Forwarding (Unicast RPF), use the **ip verify unicast source reachable-via** command in interface configuration mode. To disable Unicast RPF, use the **no** form of this command.

ip verify unicast source reachable-via {**rx** | **any**} [**allow-default**] [**allow-self-ping**] [*list*] [**12-src**] [**phys-if**]

no ip verify unicast source reachable-via

Syntax Description

rx	Examines incoming packets to determine whether the source address is in the Forwarding Information Base (FIB) and permits the packet only if the source is reachable through the interface on which the packet was received (sometimes referred to as strict mode).
any	Examines incoming packets to determine whether the source address is in the FIB and permits the packet if the source is reachable through any interface (sometimes referred to as loose mode).
allow-default	(Optional) Allows the use of the default route for RPF verification.
allow-self-ping	(Optional) Allows a router to ping its own interface or interfaces. **Caution** Use caution when enabling the **allow-self-ping** keyword. This keyword opens a denial-of-service (DoS) hole.
list	(Optional) Specifies a numbered access control list (ACL) in the following ranges: • 1 to 99 (IP standard access list) • 100 to 199 (IP extended access list) • 1300 to 1999 (IP standard access list, expanded range) • 2000 to 2699 (IP extended access list, expanded range)
l2-src	(Optional) Enables source IPv4 and source MAC address binding.
phys-if	(Optional) Enables physical input interface verification.

Command Default

Unicast RPF is disabled.

Source IPv4 and source MAC address binding is disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1(CC), 12.0	This command was introduced. This command was not included in Cisco IOS Release 11.2 or 11.3.
12.1(2)T	Added access control list (ACL) support using the *list* argument. Added per-interface statistics on dropped or suppressed packets.
12.0(15)S	This command replaced the **ip verify unicast reverse-path** command, and the following keywords were added: **allow-default**, **allow-self-ping**, **rx**, and **any**.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	The **l2-src** keyword was added to support the source IPv4 and source MAC address binding feature on Cisco 7600 series routers. The **phys-if** keyword was added to support physical input interface verification. Together, both keywords support the Unicast RPF IP and MAC Address Spoof Prevention feature.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the **ip verify unicast source reachable-via** interface command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through a router. Malformed or forged source addresses can indicate DoS attacks based on source IP address spoofing.

To use Unicast RPF, enable Cisco Express Forwarding or distributed Cisco Express Forwarding in the router. There is no need to configure the input interface for Cisco Express Forwarding. As long as Cisco Express Forwarding is running on the router, individual interfaces can be configured with other switching modes.

Note It is important for Cisco Express Forwarding to be configured globally on the router. Unicast RPF does not work without Cisco Express Forwarding.

Note Unicast RPF is an input function and is applied on the interface of a router only in the ingress direction.

When Unicast RPF is enabled on an interface, the router examines all packets that are received on that interface. The router checks to make sure that the source address appears in the FIB. If the **rx** keyword is selected, the source address must match the interface on which the packet was received. If the **any** keyword is selected, the source address must be present only in the FIB. This ability to "look backwards" is available only when Cisco Express Forwarding is enabled on the router because the lookup relies on the presence of the FIB. Cisco Express Forwarding generates the FIB as part of its operation.

Note If the source address of an incoming packet is resolved to a null adjacency, the packet will be dropped. The null interface is treated as an invalid interface by the new form of the Unicast RPF command. The older form of the command syntax did not exhibit this behavior.

Unicast RPF checks to determine whether any packet that is received at a router interface arrives on one of the best return paths to the source of the packet. If a reverse path for the packet is not found, Unicast RPF can drop or forward the packet, depending on whether an ACL is specified in the Unicast RPF command. If an ACL is specified in the command, when (and only when) a packet fails the Unicast RPF check, the ACL is checked to determine whether the packet should be dropped (using a deny statement in the ACL) or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for Unicast RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the **ip verify unicast source reachable-via** command, the router drops the forged or malformed packet immediately, and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

Unicast RPF events can be logged by specifying the logging option for the ACL entries that are used by the **ip verify unicast source reachable-via** command. Log information can be used to gather information about the attack, such as source address, time, and so on.

Strict Mode RPF

If the source address is in the FIB and reachable only through the interface on which the packet was received, the packet is passed. The syntax for this method is **ip verify unicast source reachable-via rx**.

Exists-Only (or Loose Mode) RPF

If the source address is in the FIB and reachable through any interface on the router, the packet is passed. The syntax for this method is **ip verify unicast source reachable-via any**.

Because this Unicast RPF option passes packets regardless of which interface the packet enters, it is often used on Internet service provider (ISP) routers that are “peered” with other ISP routers (where asymmetrical routing typically occurs). Packets using source addresses that have not been allocated on the Internet, which are often used for spoofed source addresses, are dropped by this Unicast RPF option. All other packets that have an entry in the FIB are passed.

allow-default

Normally, sources found in the FIB but only by way of the default route will be dropped. Specifying the **allow-default** keyword option will override this behavior. You must specify the **allow-default** keyword in the command to permit Unicast RPF to successfully match on prefixes that are known through the default route to pass these packets.

allow-self-ping

This keyword allows the router to ping its own interface or interfaces. By default, when Unicast RPF is enabled, packets that are generated by the router and destined to the router are dropped, thereby, making certain troubleshooting and management tasks difficult to accomplish. Issue the **allow-self-ping** keyword to enable self-pinging.

Caution Caution should be used when enabling the **allow-self-ping** keyword because this option opens a potential DoS hole.

Using RPF in Your Network

Use Unicast RPF strict mode on interfaces where only one path allows packets from valid source networks (networks contained in the FIB). Also, use Unicast RPF strict mode when a router has multiple paths to a given network, as long as the valid networks are switched through the incoming interfaces. Packets for invalid networks will be dropped. For example, routers at the edge of the network of an ISP

are likely to have symmetrical reverse paths. Unicast RPF strict mode is applicable in certain multihomed situations, provided that optional Border Gateway Protocol (BGP) attributes, such as weight and local preference, are used to achieve symmetric routing.

Note With Unicast RPF, all equal-cost "best" return paths are considered valid. This means that Unicast RPF works in cases where multiple return paths exist, provided that each path is equal to the others in terms of the routing cost (number of hops, weights, and so on) and as long as the route is in the FIB. Unicast RPF also functions where Enhanced Internet Gateway Routing Protocol (EIGRP) variants are being used and unequal candidate paths back to the source IP address exist.

Use Unicast RPF loose mode on interfaces where asymmetric paths allow packets from valid source networks (networks contained in the FIB). Routers that are in the core of the ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router.

IP and MAC Address Spoof Prevention on Cisco 7600 Series Routers

In Release 12.2(33)SRC and later, use the **l2-src** keyword to enable source IPv4 and source MAC address binding and the **phys-if** keyword to verify the source IP input interface. To disable source IPv4 and source MAC address binding, use the **no** form of the **ip verify unicast source reachable-via** command.The **phys-if** keyword can be used on Gigabit virtual interfaces (GVI) interfaces; the **l2-src** keyword can be used on GVI and Ethernet-like interfaces.

If an inbound packet fails either of these security checks, it will be dropped and the Unicast RPF dropped-packet counter will be incremented. The only exception occurs if a numbered access control list has been specified as part of the Unicast RPF command in strict mode, and the ACL permits the packet. In this case the packet will be forwarded and the Unicast RPF suppressed-drops counter will be incremented.

Note Neither the **12-src** nor the **phys-if** keywords can be used with the loose uRPF command, **ip verify unicast source reachable-via any** command.

Possible keyword combinations for Unicast PRF include the following:

```
allow-default
allow-self-ping
l2-src
phys-if
<ACL-number>
allow-default allow-self-ping
allow-default l2-src
allow-default phys-if
allow-default <ACL-number>
allow-self-ping l2-src
allow-self-ping phys-if
allow-self-ping <ACL-number>
l2-src phys-if
l2-src <ACL-number>
phys-if <ACL-number>
allow-default allow-self-ping l2-src
allow-default allow-self-ping phys-if
allow-default allow-self-ping <ACL-number>
allow-default l2-src phys-if
allow-default l2-src <ACL-number>
allow-default phys-if <ACL-number>
allow-self-ping l2-src phys-if
allow-self-ping l2-src <ACL-number>
```

```
allow-self-ping phys-if <ACL-number>
l2-src phys-if <ACL-number>
allow-default allow-self-ping l2-src phys-if
allow-default allow-self-ping l2-src <ACL-number>
allow-default allow-self-ping phys-if <ACL-number>
allow-default l2-src phys-if <ACL-number>
allow-self-ping l2-src phys-if <ACL-number>
allow-default allow-self-ping l2-src phys-if <ACL-number>
```

Examples

Single-homed ISP Connection with Unicast RPF

The following example uses a very simple single-homed ISP connection to demonstrate the concept of Unicast RPF. In this example, an ISP peering router is connected through a single serial interface to one upstream ISP. Hence, traffic flows into and out of the ISP will be symmetric. Because traffic flows will be symmetric, a Unicast RPF strict-mode deployment can be configured.

```
ip cef
! or "ip cef distributed" for Route Switch Processor+Versatile Interface Processor-
(RSP+VIP-) based routers.
!
interface Serial5/0/0
 description - link to upstream ISP (single-homed)
 ip address 192.168.200.225 255.255.255.252
 no ip redirects
 no ip directed-broadcasts
 no ip proxy-arp
 ip verify unicast source reachable-via
```

ACLs and Logging with Unicast RPF

The following example demonstrates the use of ACLs and logging with Unicast RPF. In this example, extended ACL 197 provides entries that deny or permit network traffic for specific address ranges. Unicast RPF is configured on interface Ethernet 0 to check packets arriving at that interface.

For example, packets with a source address of 192.168.201.10 arriving at interface Ethernet 0 are dropped because of the deny statement in ACL 197. In this case, the ACL information is logged (the logging option is turned on for the ACL entry) and dropped packets are counted per-interface and globally. Packets with a source address of 192.168.201.100 arriving at interface Ethernet 0 are forwarded because of the permit statement in ACL 197. ACL information about dropped or suppressed packets is logged (the logging option is turned on for the ACL entry) to the log server.

```
ip cef distributed
!
int eth0/1/1
 ip address 192.168.200.1 255.255.255.0
 ip verify unicast source reachable-via rx 197
!
int eth0/1/2
 ip address 192.168.201.1 255.255.255.0
!
access-list 197 deny   ip 192.168.201.0 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.64 0.0.0.63 any log-input
access-list 197 deny   ip 192.168.201.128 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.192 0.0.0.63 any log-input
access-list 197 deny ip host 0.0.0.0 any log-input
access-list 197 deny ip 172.16.0.0 0.255.255.255 any log-input
access-list 197 deny ip 10.0.0.0 0.255.255.255 any log-input
access-list 197 deny ip 172.16.0.0 0.15.255.255 any log-input
access-list 197 deny ip 192.168.0.0 0.0.255.255 any log-input
```

MAC Address Binding on Cisco 7600 Series Routers

The following example enables source IPv4 and source MAC address binding on VLAN 10.

```
Router# configure terminal
Router(config)# interface VLAN 10
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# ip verify unicast source reachable-via rx l2-src
```

Related Commands

Command	Description
ip cef	Enables Cisco Express Forwarding on the route processor card.

ip virtual-reassembly

To enable virtual fragment reassembly (VFR) on an interface, use the **ip virtual-reassembly** command in interface configuration mode. To disable VFR on an interface, use the **no** form of this command.

ip virtual-reassembly [**max-reassemblies** *number*] [**max-fragments** *number*] [**timeout** *seconds*] [**drop-fragments**]

no ip virtual-reassembly [**max-reassemblies** *number*] [**max-fragments** *number*] [**timeout** *seconds*] [**drop-fragments**]

Syntax Description

max-reassemblies *number*	(Optional) Maximum number of IP datagrams that can be reassembled at any given time. Default value: 16. If the maximum value is reached, all fragments within the following fragment set will be dropped and an alert message will be logged to the syslog server.
max-fragments *number*	(Optional) Maximum number of fragments that are allowed per IP datagram (fragment set). Default value: 32. If an IP datagram that is being reassembled receives more than the maximum allowed fragments, the IP datagram will be dropped and an alert message will be logged to the syslog server.
timeout *seconds*	(Optional) Timeout value, in seconds, for an IP datagram that is being reassembled. Default value: 3 seconds. If an IP datagram does not receive all of the fragments within the specified time, the IP datagram (and all of its fragments) will be dropped.
drop-fragments	(Optional) Enables the VFR to drop all fragments that arrive on the configured interface. By default, this function is disabled.

Defaults

VFR is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

A buffer overflow attack can occur when an attacker continuously sends a large number of incomplete IP fragments, causing the firewall to lose time and memory while trying to reassemble the fake packets.

The **max-reassemblies** *number* option and the **max-fragments** *number* option allow you to configure maximum threshold values to avoid a buffer overflow attack and to control memory usage.

In addition to configuring the maximum threshold values, each IP datagram is associated with a managed timer. If the IP datagram does not receive all of the fragments within the specified time (which can be configured via the **timeout** *seconds* option), the timer will expire and the IP datagram (and all of its fragments) will be dropped.

Automatically Enabling or Disabling VFR

VFR is designed to work with any feature that requires fragment reassembly (such as Cisco IOS Firewall and NAT). Currently, NAT enables and disables VFR internally; that is, when NAT is enabled on an interface, VFR is automatically enabled on that interface.

If more than one feature attempts to automatically enable VFR on an interface, VFR will maintain a reference count to keep track of the number of features that have enabled VFR. When the reference count is reduced to zero, VFR is automatically disabled

Examples

The following example shows how to configure VFR on interfaces ethernet2/1, ethernet2/2, and serial3/0 to facilitate the firewall that is enabled in the outbound direction on interface serial3/0. In this example, the firewall rules that specify the list of LAN1 and LAN2 originating protocols (FTP, HTTP and SMTP) are to be inspected.

```
ip inspect name INTERNET-FW ftp
ip inspect name INTERNET-FW http
ip inspect name INTERNET-FW smtp!
!
interface Loopback0
 ip address 10.0.1.1 255.255.255.255
!
interface Ethernet2/0
 ip address 10.4.21.9 255.255.0.0
 no ip proxy-arp
 no ip mroute-cache
 duplex half
 no cdp enable
!
interface Ethernet2/1
 description LAN1
 ip address 10.4.0.2 255.255.255.0
 ip virtual-reassembly
 duplex half
!
interface Ethernet2/2
 description LAN2
 ip address 10.15.0.2 255.255.255.0
 ip virtual-reassembly
 duplex half
!
interface Ethernet2/3
 no ip address
 no ip mroute-cache
 shutdown
 duplex half
!
interface Serial3/0
 description Internet
 ip unnumbered Loopback0
 encapsulation ppp
 ip access-group 102 in
 ip inspect INTERNET-FW out
 ip virtual-reassembly
 serial restart-delay 0
```

Related Commands

Command	Description
show ip virtual-reassembly	Displays the configuration and statistical information of the VFR on a given interface.

ip vrf

To define a VPN routing and forwarding (VRF) instance and to enter VRF configuration mode, use the **ip vrf** command in global configuration mode. To remove a VRF instance, use the **no** form of this command.

ip vrf *vrf-name*

no ip vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

No VRFs are defined. No import or export lists are associated with a VRF. No route maps are associated with a VRF.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The **ip vrf** *vrf-name* command creates a VRF instance named *vrf-name*. To make the VRF functional, a route distinguisher (RD) must be created using the **rd** *route-distinguisher* command in VRF configuration mode. The **rd** *route-distinguisher* command creates the routing and forwarding tables and associates the RD with the VRF instance named *vrf-name*.

The **ip vrf default** command can be used to configure a VRF instance that is a NULL value until a default VRF name can be configured. This is typically before any VRF related AAA commands are configured.

Examples

The following example shows how to import a route map to a VRF instance named VPN1:

```
ip vrf vpn1
 rd 100:2
 route-target both 100:2
 route-target import 100:1
```

Related Commands

Command	Description
ip vrf forwarding (**interface configuration**)	Associates a VRF with an interface or subinterface.
rd	Creates routing and forwarding tables for a VRF and specifies the default route distinguisher for a VPN.

ip vrf forwarding

To associate a Virtual Private Network (VPN) routing and forwarding (VRF) instance with a Diameter peer, use the **ip vrf forwarding** command in Diameter peer configuration mode. To enable Diameter peers to use the global (default) routing table, use the **no** form of this command.

ip vrf forwarding *name*

no ip vrf forwarding *name*

Syntax Description

name	Name assigned to a VRF.

Command Default

Diameter peers use the global routing table.

Command Modes

Diameter peer configuration (config-dia-peer)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(54)SG	This command was integrated into Cisco IOS Release 12.2(54)SG.

Usage Guidelines

Use the **ip vrf forwarding** command to specify a VRF for a Diameter peer. If a VRF name is not configured for a Diameter server, the global routing table will be used.

If the VRF associated with the specified name has not been configured, the command will have no effect and this error message will appear: **No VRF found with the name** *name*.

Examples

The following example shows how to configure the VRF for a Diameter peer:

```
Router (config-dia-peer)# ip vrf forwarding diam_peer_1
```

Related Commands

Command	Description
diameter peer	Configures a Diameter peer and enters Diameter peer configuration submode.
ip vrf forwarding (server-group)	Configures the VRF reference of an AAA RADIUS or TACACS+ server group.

ip vrf forwarding (server-group)

To configure the Virtual Private Network (VPN) routing and forwarding (VRF) reference of an authentication, authorization, and accounting (AAA) RADIUS or TACACS+ server group, use the **ip vrf forwarding** command in server-group configuration mode. To enable server groups to use the global (default) routing table, use the **no** form of this command.

ip vrf forwarding *vrf-name*

no ip vrf forwarding *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

Server groups use the global routing table.

Command Modes

Server-group configuration (server-group)

Command History

Release	Modification
12.2(2)DD	This command was introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(7)T	Functionality was added for TACACS+ servers.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA1	This command was integrated into Cisco IOS Release 12.2(33)SRA1.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **ip vrf forwarding** command to specify a VRF for a AAA RADIUS or TACACS+ server group. This command enables dial users to utilize AAA servers in different routing domains.

Examples

The following example shows how to configure the VRF user to reference the RADIUS server in a different VRF server group:

```
aaa group server radius sg_global
 server-private 172.16.0.0 timeout 5 retransmit 3
!
aaa group server radius sg_water
 server-private 10.10.0.0 timeout 5 retransmit 3 key water
 ip vrf forwarding water
```

The following example shows how to configure the VRF user to reference the TACACS+ server in the server group tacacs1:

```
aaa group server tacacs+tacacs1
    server-private 10.1.1.1 port 19 key cisco
    ip vrf forwarding cisco
    ip tacacs source-interface Loopback0

  ip vrf cisco
   rd 100:1

  interface Loopback0
   ip address 10.0.0.2 255.0.0.0
   ip vrf forwarding cisco
```

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
ip tacacs source-interface	Uses the IP address of a specified interface for all outgoing TACACS+ packets.
ip vrf forwarding (server-group)	Configures the VRF reference of an AAA RADIUS or TACACS+ server group.
server-private	Configures the IP address of the private RADIUS server for the group server.

ip wccp web-cache accelerated

To enable the hardware acceleration for WCCP version 1, use the **ip wccp web-cache accelerated** command in global configuration mode. To disable hardware acceleration, use the **no** form of this command.

ip wccp web-cache accelerated [[**group-address** *group-address*] | [**redirect-list** *access-list*] | [**group-list** *access-list*] | [**password** *password*]]

no ip wccp web-cache accelerated

Syntax Description

group-address *group-address*	(Optional) Directs the router to use a specified multicast IP address for communication with the WCCP service group. See the "Usage Guidelines" section for additional information.
redirect-list *access-list*	(Optional) Directs the router to use an access list to control traffic that is redirected to this service group. See the "Usage Guidelines" section for additional information.
group-list *access-list*	(Optional) Directs the router to use an access list to determine which cache engines are allowed to participate in the service group. See the "Usage Guidelines" section for additional information.
password *password*	(Optional) Specifies a string that directs the router to apply MD5 authentication to messages received from the service group specified by the service name given. See the "Usage Guidelines" section for additional information.

Defaults

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(18)SXD1	This command was changed to support the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.

Usage Guidelines

This command is supported on software releases later than cache engine software Release ACNS 4.2.1.

The **group-address** *group-address* option requires a multicast address that is used by the router to determine which cache engine should receive redirected messages. This option instructs the router to use the specified multicast IP address to coalesce the "I See You" responses for the "Here I Am" messages

that it has received on this group address. In addition, the response is sent to the group address. The default is for no **group-address** to be configured, so that all "Here I Am" messages are responded to with a unicast reply.

The **redirect-list** *access-list* option instructs the router to use an access list to control the traffic that is redirected to the cache engines of the service group that is specified by the service-name given. The *access-list* argument specifies either a number from 1 to 99 to represent a standard or extended access-list number, or a name to represent a named standard or extended access list. The access list itself specifies the traffic that is permitted to be redirected. The default is for no **redirect-list** to be configured (all traffic is redirected).

The **group-list** *access-list* option instructs the router to use an access list to control the cache engines that are allowed to participate in the specified service group. The *access-list* argument specifies either a number from 1 to 99 to represent a standard access-list number, or a name to represent a named standard access list. The access list specifies which cache engines are permitted to participate in the service group. The default is for no **group-list** to be configured, so that all cache engines may participate in the service group.

The password can be up to seven characters. When you designate a password, the messages that are not accepted by the authentication are discarded. The password name is combined with the HMAC MD5 value to create security for the connection between the router and the cache engine.

Examples

The following example shows how to enable the hardware acceleration for WCCP version 1:

```
Router(config)# ip wccp web-cache accelerated
```

Related Commands

Command	Description
ip wccp version	Specifies which version of WCCP to configure on your router.

ips signature update cisco

To initiate a one-time download of Cisco IOS Intrusion Prevention System (IPS) signatures from Cisco.com, use the **ips signature update cisco** command in Privileged EXEC mode.

ips signature update cisco {**next** | **latest** | *signature*} [**username** *name* **password** *password*]

Syntax Description

next	Specifies the next signature file version from the current signature file on the router.
latest	Specifies the IOS IPS to search for the latest signature file.
signature	This argument specifies a specific signature file on Cisco.com.
username *name*	Defines the username for the automatic signature update function.
password *password*	Defines the password for the automatic signature update function.

Defaults

Privileged EXEC mode (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

The **ips signature update cisco** command is used to initiate a one-time download of IPS signatures from Cisco.com. If you want IPS signatures to be periodically downloaded from Cisco.com, use the **ip ips auto-update** command in global configuration mode and subsequently the **cisco** command in IPS-auto-update configuration mode to enable automatic signature updates from Cisco.com.

If the *username* and *password* is not specified, then the username and password that is specified in the IPS auto update configuration is used. A user name and password must be configured for updating signatures directly from Cisco.com.

Examples

The following example shows how to get the latest automatic signature update from Cisco.com:

```
Router# ips signature update cisco latest
```

Related Commands

Command	Description
ip ips auto-update	Enables automatic signature updates for Cisco IOS IPS.
cisco	Enables automatic signature updates from Cisco.com.

ipv4 (ldap)

To create an IPv4 address within a Lightweight Directory Access Protocol (LDAP) server address pool, use the **ipv4** command in LDAP server configuration mode. To delete an IPv4 address within an LDAP server address pool, use the **no** form of this command.

ipv4 *ipv4-address*

no ipv4 *ipv4-address*

Syntax Description

ipv4-address	IPv4 address of the LDAP server.

Command Default

No IPv4 addresses are created in the LDAP server address pool.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Examples

The following example shows how to create an IPv4 address in an LDAP server address pool:

```
Router(config)# ldap server server1
Router(config-ldap-server)# ipv4 10.0.0.1
```

Related Commands

Command	Description
ldap server	Defines an LDAP server and enters LDAP server configuration mode.
transport port (**ldap**)	Configures the transport protocol for establishing a connection with the LDAP server.

ipv6 crypto map

To enable an IPv6 crypto map on an interface, use the **ipv6 crypto map** command in interface configuration mode. To disable, use the **no** form of this command.

ipv6 crypto map *map-name*

no ipv6 crypto map

Syntax Description

map-name	Identifies the crypto map set.

Command Default

No IPv6 crypto maps are enabled on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(4)M	This command was introduced.

Usage Guidelines

This command differentiates IPv6 and IPv4 crypto maps.

Examples

The following example shows how to enable an IPv6 crypto map on an interface:

```
Router# configure terminal
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 crypto map CM_V4
```

Related Commands

Command	Description
crypto map (global IPsec)	Creates or modifies a crypto map entry.

isakmp authorization list

To configure an Internet Key Exchange (IKE) shared secret using the authentication, authorization, and accounting (AAA) server in an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **isakmp authorization list** command in ISAKMP profile configuration mode. To disable the shared secret, use the **no** form of this command.

isakmp authorization list *list-name*

no isakmp authorization list *list-name*

Syntax Description

list-name	AAA authorization list used for configuration mode attributes or preshared keys for aggressive mode.

Defaults

No default behaviors or values

Command Modes

ISAKMP profile configuration (config-isa-prof)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.2(33)SRA.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

This command allows you to retrieve a shared secret from an AAA server.

Examples

The following example shows that an IKE shared secret is configured using an AAA server on a router:

```
crypto isakmp profile vpnprofile
 isakmp authorization list ikessaaalist
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.

issuer-name

To specify the distinguished name (DN) as the certification authority (CA) issuer name for the certificate server, use the **issuer-name** command in certificate server configuration mode. To clear the issuer name and return to the default, use the **no** form of this command.

issuer-name *DN-string*

no issuer-name *DN-string*

Syntax Description

DN-string	Name of the DN string.

Defaults

If the issuer name is not configured, **CN** = *cs-label*

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The DN-string value cannot be changed after the certificate server generates its signed certificate.

Examples

The following example shows how to define an issuer name for the certificate server "mycertserver":

```
Router(config)# ip http server
Router(config)# crypto pki server mycertserver
Router(cs-server)# database level minimal
Router(cs-server)# database url nvram:
Router(cs-server)# issuer-name CN = ipsec_cs,L = My Town,C = US
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.

ivrf

To specify a user-defined VPN routing and forwarding (VRF) or use the global VRF, use the **ivrf** command in IKEv2 profile configuration mode. To delete the VRF specification, use the **no** form of this command.

ivrf *name*

no ivrf

Syntax Description

name	VRF name.

Command Default

VRF is not specified.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to specify a user-defined VRF or a global VRF, which should be attached to static and dynamic crypto maps. The inside VRF (IVRF) for a tunnel interface should be configured on the tunnel interface. IVRF specifies the VRF for cleartext packets. The default value for IVRF is Forward VRF (FVRF).

Examples

The following example shows how to specify IVRF:

```
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# ivrf vrf1
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.
show crypto ikev2 profile	Displays the IKEv2 profile.

keepalive (isakmp profile)

To allow the gateway to send dead peer detection (DPD) messages to the peer, use the **keepalive** command in Internet Security Association Key Management Protocol (ISAKMP) profile configuration mode. To return to the default, use the **no** form of this command.

keepalive *seconds* **retry** *retry-seconds*

no keepalive *seconds* **retry** *retry-seconds*

Syntax Description

seconds	Number of seconds between DPD messages. The range is from 10 to 3600 seconds.
retry *retry-seconds*	Number of seconds between retries if DPD message fails. The range is from 2 to 60 seconds.

Defaults

If this command is not configured, a DPD message is not sent to the client.

Command Modes

ISAKMP profile configuration (config-isa-prof)

Command History

Release	Modification
12.2(15)T	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Use this command to enable the gateway (instead of the client) to send DPD messages to the client. Internet Key Exchange (IKE) DPD is a new keepalive scheme that sends messages to let the router know that the client is still connected.

Examples

The following example shows that DPD messages have been configured to be sent every 60 seconds and every 5 seconds between retries if the peer does not respond:

```
crypto isakmp profile vpnprofile
 keepalive 60 retry 5
```

kerberos clients mandatory

To cause the **rsh**, **rcp**, **rlogin**, and **telnet** commands to fail if they cannot negotiate the Kerberos protocol with the remote server, use the **kerberos clients mandatory** command in global configuration mode. To make Kerberos optional, use the **no** form of this command.

kerberos clients mandatory

no kerberos clients mandatory

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If this command is not configured and the user has Kerberos credentials stored locally, the **rsh**, **rcp**, **rlogin**, and **telnet** commands attempt to negotiate the Kerberos protocol with the remote server and will use the non-Kerberized protocols if unsuccessful.

If this command is not configured and the user has no Kerberos credentials, the standard protocols for **rcp** and **rsh** are used to negotiate.

Examples

The following example causes the **rsh**, **rcp**, **rlogin**, and **telnet** commands to fail if they cannot negotiate the Kerberos protocol with the remote server:

```
kerberos clients mandatory
```

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
kerberos credentials forward	Forces all network application clients on the router to forward the Kerberos credentials of users upon successful Kerberos authentication.
rlogin	Logs in to a UNIX host using rlogin.

Command	Description
rsh	Executes a command remotely on a remote rsh host.
telnet	Logs in to a host that supports Telnet.

kerberos credentials forward

To force all network application clients on the router to forward users' Kerberos credentials upon successful Kerberos authentication, use the **kerberos credentials forward** command in global configuration mode. To turn off forwarding of Kerberos credentials, use the **no** form of this command.

kerberos credentials forward

no kerberos credentials forward

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Enable credentials forwarding to have users' ticket granting tickets (TGTs) forwarded to the host on which they authenticate. In this way, users can connect to multiple hosts in the Kerberos realm without running the KINIT program each time they need to get a TGT.

Examples

The following example forces all network application clients on the router to forward users' Kerberos credentials upon successful Kerberos authentication:

```
kerberos credentials forward
```

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
rlogin	Logs in to a UNIX host using rlogin.
rsh	Executes a command remotely on a remote rsh host.
telnet	Logs in to a host that supports Telnet.

kerberos instance map

To map Kerberos instances to Cisco IOS privilege levels, use the **kerberos instance map** command in global configuration mode. To remove a Kerberos instance map, use the **no** form of this command.

kerberos instance map *instance privilege-level*

no kerberos instance map *instance*

Syntax Description

instance	Name of a Kerberos instance.
privilege-level	The privilege level at which a user is set if the user's Kerberos principal contains the matching Kerberos instance. You can specify up to 16 privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges.

Defaults

Privilege level 1

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to create user instances with access to administrative commands.

Examples

The following example sets the privilege level to 15 for authenticated Kerberos users with the *admin* instance in Kerberos realm:

```
kerberos instance map admin 15
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.

kerberos local-realm

To specify the Kerberos realm in which the router is located, use the **kerberos local-realm** command in global configuration mode. To remove the specified Kerberos realm from this router, use the **no** form of this command.

kerberos local-realm *kerberos-realm*

no kerberos local-realm

Syntax Description

kerberos-realm	The name of the default Kerberos realm. A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase characters.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The router can be located in more than one realm at a time. However, there can only be one instance of Kerberos local-realm. The realm specified with this command is the default realm.

Examples

The following example specify the Kerberos realm in which the router is located as EXAMPLE.COM:

```
kerberos local-realm EXAMPLE.COM
```

Related Commands

Command	Description
kerberos preauth	Specifies a preauthentication method to use to communicate with the KDC.
kerberos realm	Maps a host name or DNS domain to a Kerberos realm.
kerberos server	Specifies the location of the Kerberos server for a given Kerberos realm.
kerberos srvtab entry	Specifies a krb5 SRVTAB entry.
kerberos srvtab remote	Retrieves a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration.

kerberos password

To set the password shared with the key distribution center, use the **kerberos password** command in global configuration mode. To disable the configured password, use the **no** form of this command.

kerberos password [*text-string*]

no kerberos password [*text-string*]

Syntax Description

text-string	(Optional) The password string.

Command Default

The password is not set.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRB.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Kerberos is a network authentication protocol that allows a secured way of node communication in a nonsecure network.

Examples

The following example shows how to set the password:

```
Router# configure terminal
Router(config)# kerberos password treas123
```

Related Commands

Command	Description
kerberos clients mandatory	Specifies the default direction of filters from RADIUS.
kerberos credentials forward	Forces all network application clients on the router to forward the Kerberos credentials of users upon successful Kerberos authentication.

kerberos preauth

To specify a preauthentication method to use to communicate with the key distribution center (KDC), use the **kerberos preauth** command in global configuration mode. To disable Kerberos preauthentication, use the **no** form of this command.

kerberos preauth [**encrypted-unix-timestamp** | **encrypted-kerberos-timestamp** | **none**]

no kerberos preauth

Syntax Description

encrypted-unix-timestamp	(Optional) Use an encrypted UNIX timestamp as a quick authentication method when communicating with the KDC.
encrypted-kerberos-timestamp	(Optional) Use the RFC1510 kerberos timestamp as a quick authentication method when communicating with the KDC.
none	(Optional) Do not use Kerberos preauthentication.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

It is more secure to use a preauthentication for communications with the KDC. However, communication with the KDC will fail if the KDC does not support this particular version of **kerberos preauth.** If that happens, turn off the preauthentication with the **none** option.

The **no** form of this command is equivalent to using the **none** keyword.

Examples

The following example enables Kerberos preauthentication:

```
kerberos preauth encrypted-unix-timestamp
```

The following example disables Kerberos preauthentication:

```
kerberos preauth none
```

Related Commands

Command	Description
kerberos local-realm	Specifies the Kerberos realm in which the router is located.
kerberos server	Specifies the location of the Kerberos server for a given Kerberos realm.
kerberos srvtab entry	Specifies a krb5 SRVTAB entry.
kerberos srvtab remote	Retrieves a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration.

kerberos processes

To set the number of kerberos processes to service requests, use the **kerberos processes** command in global configuration mode. To disable the configuration, use the **no** form of this command.

kerberos processes *number*

no kerberos processes

Syntax Description

number	Number of processes. The range is from 1 to 10. The default is 1.

Command Default

The default process is 1.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows how to set the number of kerberos processes to 10:

```
Router# configure terminal
Router(config)# kerberos processes 10
```

Related Commands

Command	Description
debug kerberos	Displays information associated with the Kerberos Authentication Subsystem.

kerberos realm

To map a host name or Domain Name System (DNS) domain to a Kerberos realm, use the **kerberos realm** command in global configuration mode. To remove a Kerberos realm map, use the **no** form of this command.

kerberos realm {*dns-domain* | *host*} *kerberos-realm*

no kerberos realm {*dns-domain* | *host*} *kerberos-realm*

Syntax Description

dns-domain	Name of a DNS domain or host.
host	Name of a DNS host.
kerberos-realm	Name of the Kerberos realm to which the specified domain or host belongs.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

DNS domains are specified with a leading dot (.) character; host names cannot begin with a dot (.) character. There can be multiple entries of this line.

A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase characters. The router can be located in more than one realm at a time. Kerberos realm names must be in all uppercase characters.

Examples

The following example maps the domain name “example.com” to the Kerberos realm, EXAMPLE.COM:

```
kerberos realm .example.com EXAMPLE.COM
```

Related Commands

Command	Description
kerberos local-realm	Specifies the Kerberos realm in which the router is located.
kerberos server	Specifies the location of the Kerberos server for a given Kerberos realm.

Command	Description
kerberos srvtab entry	Specifies a krb5 SRVTAB entry.
kerberos srvtab remote	Retrieves a SRVTAB file from a remote host and automatically generates a Kerberos SRVTAB entry configuration.

kerberos retry

To configure the number of retry attempts for the key distribution center (KDC) sessions, use the **kerberos retry** command in global configuration mode. To return to the default setting (4 retries), use the **no** form of this command.

kerberos retry *number*

no kerberos retry

Syntax Description

number	Number of retry attempts. The range is from 1 to 5. The default value is 4.

Command Default

The default value is four retry attempts.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

When multiple KDCs are configured, there is no way to control the timeout so that failover occurs. This causes common client applications to fail before the next KDC is contacted. Therefore, the kerberos retry command enables you to establish stable communication with the KDCs.

Examples

The following example shows how to configure the retry value for the KDC session:

```
Router> enable
Router# configure terminal
Router(config)# kerberos retry 3
```

Related Commands

Command	Description
kerberos clients mandatory	Causes the **rsh**, **rcp**, **rlogin**, and **telnet** commands to fail if they cannot negotiate the Kerberos protocol with the remote server.
kerberos credentials forward	Forces all network application clients on the router to forward users' Kerberos credentials upon successful Kerberos authentication.

kerberos server

To specify the location of the Kerberos server for a given Kerberos realm, use the **kerberos server** command in global configuration mode. To remove a Kerberos server for a specified Kerberos realm, use the **no** form of this command.

kerberos server *kerberos-realm* {*host-name* | *ip-address*} [*port-number*]

no kerberos server *kerberos-realm* {*host-name* | *ip-address*}

Syntax Description

kerberos-realm	Name of the Kerberos realm. A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase letters.
host-name	Name of the host functioning as a Kerberos server for the specified Kerberos realm (translated into an IP address at the time of entry).
ip-address	IP address of the host functioning as the Kerberos server for the specified Kerberos realm.
port-number	(Optional) Port that the key distribution center (KDC) monitors (defaults to 88).

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **kerberos server** command to specify the location of the Kerberos server for a given realm.

Examples

The following example specifies 192.168.47.66 as the Kerberos server for the Kerberos realm EXAMPLE.COM:

```
kerberos server EXAMPLE.COM 192.168.47.66
```

Related Commands

Command	Description
kerberos local-realm	Specifies the Kerberos realm in which the router is located.
kerberos realm	Maps a host name or DNS domain to a Kerberos realm.
kerberos srvtab entry	Specifies a krb5 SRVTAB entry.
kerberos srvtab remote	Retrieves a SRVTAB file from a remote host and automatically generates a Kerberos SRVTAB entry configuration.

kerberos srvtab entry

To retrieve a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration, use the **kerberos srvtab entry** command in global configuration mode. To remove a SRVTAB entry from the router's configuration, use the **no** form of this command.

kerberos srvtab entry *kerberos-principal principal-type timestamp key-version number key-type key-length encrypted-keytab*

no kerberos srvtab entry *kerberos-principal principal-type*

Syntax Description

kerberos-principal	A service on the router.
principal-type	Version of the Kerberos SRVTAB.
timestamp	Number representing the date and time the SRVTAB entry was created.
key-version number	Version of the encryption key format.
key-type	Type of encryption used.
key-length	Length, in bytes, of the encryption key.
encrypted-keytab	Secret key the router shares with the key distribution center (KDC). It is encrypted with the private Data Encryption Standard (DES) key (if available) when you write out your configuration.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When you use the **kerberos srvtab remote** command to copy the SRVTAB file from a remote host (generally the KDC), it parses the information in this file and stores it in the router's running configuration in the **kerberos srvtab entry** format. The key for each SRVTAB entry is encrypted with a private DES key if one is defined on the router. To ensure that the SRVTAB is available (that is, that it does not need to be acquired from the KDC) when you reboot the router, use the **write memory** router configuration command to write the router's running configuration to NVRAM.

If you reload a configuration, with a SRVTAB encrypted with a private DES key, on to a router that does not have a private DES key defined, the router displays a message informing you that the SRVTAB entry has been corrupted, and discards the entry.

If you change the private DES key and reload an old version of the router's configuration that contains SRVTAB entries encrypted with the old private DES keys, the router will restore your Kerberos SRVTAB entries, but the SRVTAB keys will be corrupted. In this case, you must delete your old Kerberos SRVTAB entries and reload your Kerberos SRVTABs on to the router using the **kerberos srvtab remote** command.

Although you can configure **kerberos srvtab entry** on the router manually, generally you would not do this because the keytab is encrypted automatically by the router when you copy the SRVTAB using the **kerberos srvtab remote** command.

Examples

In the following example, host/new-router.example.com@EXAMPLE.COM is the host, 0 is the type, 817680774 is the timestamp, 1 is the version of the key, 1 indicates the DES is the encryption type, 8 is the number of bytes, and .cCN.YoU.okK is the encrypted key:

```
kerberos srvtab entry host/new-router.example.com@EXAMPLE.COM 0 817680774 1 1 8
.cCN.YoU.okK
```

Related Commands

Command	Description
kerberos srvtab remote	Retrieves a krb5 SRVTAB file from the specified host.
key config-key	Defines a private DES key for the router.

kerberos srvtab remote

To retrieve a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration, use the **kerberos srvtab remote** command in global configuration mode.

kerberos srvtab remote {boot_device:*URL*}

Syntax Description

URL	Machine that has the Kerberos SRVTAB file.
ip-address	IP address of the machine that has the Kerberos SRVTAB file.
filename	Name of the SRVTAB file.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When you use the **kerberos srvtab remote** command to copy the SRVTAB file from the remote host (generally the key distribution center [KDC]), it parses the information in this file and stores it in the router's running configuration in the **kerberos srvtab entry** format. The key for each SRVTAB entry is encrypted with the private Data Encryption Standard (DES) key if one is defined on the router. To ensure that the SRVTAB is available (that is, that it does not need to be acquired from the KDC) when you reboot the router, use the **write memory** configuration command to write the router's running configuration to NVRAM.

Examples

The following example copies the SRVTAB file residing on b1.example.com to a router named s1.example.com:

```
kerberos srvtab remote tftp://b1.example.com/s1.example.com-new-srvtab
```

Related Commands

Command	Description
kerberos srvtab entry	Retrieves a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration.
key config-key	Defines a private DES key for the router.

kerberos timeout

To configure the timeout for key distribution center (KDC) requests, use the **kerberos timeout** command in global configuration mode. To return to the default setting (5 seconds), use the **no** form of this command.

kerberos timeout *seconds*

no kerberos timeout

Syntax Description

seconds	Timeout, in seconds, for KDC requests. The value range is from 1 to 10. The default value is 5 seconds.

Command Default

The timeout for KDC requests is 5 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

When multiple KDCs are configured, there is no way to control the timeout so that failover occurs. This causes common client applications to fail before the next KDC is contacted. Therefore, the kerberos retry command enables you to establish stable communication with the KDCs.

Examples

The following example shows how to configure the timeout value for KDC requests:

```
Router> enable
Router# configure terminal
Router(config)# kerberos timeout 3
```

Related Commands

Command	Description
kerberos clients mandatory	Causes the **rsh**, **rcp**, **rlogin**, and **telnet** commands to fail if they cannot negotiate the Kerberos protocol with the remote server.
kerberos credentials forward	Forces all network application clients on the router to forward users' Kerberos credentials upon successful Kerberos authentication.

key (isakmp-group)

To specify the Internet Key Exchange (IKE) preshared key for group policy attribute definition, use the **key** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove a preshared key, use the **no** form of this command.

key *name*

no key *name*

Syntax Description

name	IKE preshared key that matches the password entered on the client. **Note** This value must match the "password" field that is defined in the Cisco VPN Client 3.x configuration GUI.

Defaults

No default behavior or values.

Command Modes

ISAKMP group configuration (config-isakmp-group)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **key** command to specify the IKE preshared key when defining group policy information for Mode Configuration push. (It follows the **crypto isakmp client configuration group** command.) You *must* configure this command if the client identifies itself to the router with a preshared key. (You do not have to enable this command if the client uses a certificate for identification.)

Examples

The following example shows how to specify the preshared key "cisco":

```
crypto isakmp client configuration group default
  key cisco
  dns 10.2.2.2 10.3.2.3
  pool dog
  acl 199
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto isakmp client configuration group	Specifies the DNS domain to which a group belongs.

key config-key

To define a private DES key for the router, use the **key config-key** command in global configuration mode. To delete a private Data Encryption Standard (DES) key from the router, use the **no** form of this command.

key config-key 1 *string*

no key config-key 1 *string*

Syntax Description

1	Key number. This number is always 1.
string	Private DES key (can be up to eight alphanumeric characters).

Defaults

No DES-key defined.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was released.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command defines a private DES key for the router that will not show up in the router configuration. This private DES key can be used to DES-encrypt certain parts of the router's configuration.

Caution The private DES key is unrecoverable. If you encrypt part of your configuration with the private DES key and lose or forget the key, you will not be able to recover the encrypted data.

Examples

The following example sets *keyxx* as the private DES key on the router:

```
key config-key 1 keyxx
```

Related Commands

Command	Description
kerberos srvtab entry	Specifies a krb5 SRVTAB entry.
kerberos srvtab remote	Retrieves a SRVTAB file from a remote host and automatically generates a Kerberos SRVTAB entry configuration.

key config-key password-encryption

To store a type 6 encryption key in private NVRAM, use the **key config-key password-encryption** command in global configuration mode. To disable the encryption, use the **no** form of this command.

key config-key password-encryption [*text*]

no key config-key password-encryption [*text*]

Syntax Description

text	(Optional) Password or master key. **Note** It is recommended that you do not use the *text* argument but instead use interactive mode (using the enter key after you enter the **key config-key password-encryption** command) so that the preshared key will not be printed anywhere and, therefore, cannot be seen.

Defaults

No type 6 password encryption

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

You can securely store plain text passwords in type 6 format in NVRAM using a command-line interface (CLI). Type 6 passwords are encrypted. Although the encrypted passwords can be seen or retrieved, it is difficult to decrypt them to find out the actual password. Use the **key config-key password-encryption** command with the **password encryption aes** command to configure and enable the password (symmetric cipher Advanced Encryption Standard [AES] is used to encrypt the keys). The password (key) configured using the **key config-key password-encryption** command is the master encryption key that is used to encrypt all other keys in the router.

If you configure the **password encryption aes** command without configuring the **key config-key password-encryption** command, the following message is printed at startup or during any nonvolatile generation (NVGEN) process, such as when the **show running-config** or **copy running-config startup-config** commands have been configured:

```
"Can not encrypt password. Please configure a configuration-key with 'key config-key'"
```

Changing a Password

If the password (master key) is changed, or reencrypted, using the **key config-key password-encryption** command), the list registry passes the old key and the new key to the application modules that are using type 6 encryption.

Deleting a Password

If the master key that was configured using the **key config-key password-encryption** command is deleted from the system, a warning is printed (and a confirm prompt is issued) that states that all type 6 passwords will become useless. As a security measure, after the passwords have been encrypted, they will never be decrypted in the Cisco IOS software. However, passwords can be reencrypted as explained in the previous paragraph.

Caution If the password configured using the **key config-key password-encryption** command is lost, it cannot be recovered. The password should be stored in a safe location.

Unconfiguring Password Encryption

If you later unconfigure password encryption using the **no password encryption aes** command, all existing type 6 passwords are left unchanged, and as long as the password (master key) that was configured using the **key config-key password-encryption** command exists, the type 6 passwords will be decrypted as and when required by the application.

Storing Passwords

Because no one can "read" the password (configured using the **key config-key password-encryption** command), there is no way that the password can be retrieved from the router. Existing management stations cannot "know" what it is unless the stations are enhanced to include this key somewhere, in which case the password needs to be stored securely within the management system. If configurations are stored using TFTP, the configurations are not standalone, meaning that they cannot be loaded onto a router. Before or after the configurations are loaded onto a router, the password must be manually added (using the **key config-key password-encryption** command). The password can be manually added to the stored configuration but is not recommended because adding the password manually allows anyone to decrypt all passwords in that configuration.

Configuring New or Unknown Passwords

If you enter or cut and paste cipher text that does not match the master key, or if there is no master key, the cipher text is accepted or saved, but an alert message is printed. The alert message is as follows:

```
"ciphertext>[for username bar>] is incompatible with the configured master key."
```

If a new master key is configured, all the plain keys are encrypted and made type 6 keys. The existing type 6 keys are not encrypted. The existing type 6 keys are left as is.

If the old master key is lost or unknown, you have the option of deleting the master key using the **no key config-key password-encryption** command. Deleting the master key using the **no key config-key password-encryption** command causes the existing encrypted passwords to remain encrypted in the router configuration. The passwords will not be decrypted.

Examples

The following example shows that a type 6 encryption key is to be stored in NVRAM:

```
Router (config)# key config-key password-encryption
```

Related Commands

Command	Description
password encryption aes	Enables a type 6 encrypted preshared key.
password logging	Provides a log of debugging output for a type 6 password operation.

keyring

To configure a keyring with an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **keyring** command in ISAKMP profile configuration mode. To remove the keyring from the ISAKMP profile, use the **no** form of this command.

keyring *keyring-name*

no keyring *keyring-name*

Syntax Description

keyring-name	The keyring name, which must match the keyring name that was defined in the global configuration.

Defaults

If this command is not used, the ISAKMP profile uses the keys defined in the global configuration.

Command Modes

ISAKMP profile configuration (config-isa-prof)

Command History

Release	Modification
12.2(15)T	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The ISAKMP profile successfully completes authentication of peers if the peer keys are defined in the keyring that is attached to this profile. If no keyring is defined in the profile, the global keys that were defined in the global configuration are used.

Examples

The following example shows that “vpnkeyring” is configured as the keyring name:

```
crypto isakmp profile vpnprofile
 keyring vpnkeyring
```

keyring (IKEv2 profile)

To specify a locally defined or accounting, authentication and authorization (AAA)-based keyring, use the **keyring** command in IKEv2 profile configuration mode. To delete the keyring, use the **no** form of this command.

keyring [**aaa**] *name*

no keyring

Syntax Description

aaa	(Optional) Specifies the AAA-based preshared keys list name.
name	The keyring name for a locally defined keyring or AAA method list for an AAA-based keyring.

Command Default

A keyring is not specified.

Command Modes

IKEv2 profile configuration (crypto-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to specify a keyring for use with the local and remote preshared key authentication methods. Only one keyring can be configured either local or AAA based.

Note Local AAA is not supported for AAA-based preshared keys.

Examples

The following example shows how to configure an AAA-based keyring and assign the keyring to a profile:

```
Router(config)# aaa new-model
Router(config)# aaa authentication login aaa-psk-list default group radius
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# keyring aaa aaa-psk-list
```

The following example shows how to configure a locally defined keyring:

```
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# keyring keyring1
```

Related Commands

Command	Description
crypto ikev2 keyring	Defines an IKEv2 keyring.

key-string (IKE)

To specify the Rivest, Shamir, and Adelman (RSA) public key of the remote peer, use the **key-string** command in public key configuration mode. To remove the RSA public key, use the **no** form of this command.

key-string *key-string*

no key-string *key-string*

Syntax Description

key-string	Enter the key in hexadecimal format. While entering the key data, you can press Return to continue entering data.

Defaults

No default behavior or values

Command Modes

Public key configuration (config-pubkey)

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Before using this command, you must enter the **rsa-pubkey** command in the crypto keyring mode.

If possible, to avoid mistakes, you should cut and paste the key data (instead of attempting to type in the data).

To complete the command, you must return to the global configuration mode by typing **quit** at the config-pubkey prompt.

Examples

The following example manually specifies the RSA public keys of an IP Security (IPSec) peer:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```

Related Commands

Command	Description
crypto keyring	Defines a crypto keyring.
rsa-pubkey	Defines the RSA public key to be used for encryption or signatures during IKE authentication.
show crypto keyring	Displays keyrings on your router.

language

To specify the language to be used in a webvpn context, use the **language** command in webvpn context configuration mode. To remove the language, use the **no** form of this command.

language {**Japanese** | **customize** *language-name device*:*file*}

no language {**Japanese** | **customize** *language-name device*:*file*}

Syntax Descriptionn

Japanese	Specifies that the language to be used is Japanese.
customize *language-name device*:*file*	Specifies that a language other than English or Japanese is to be used. • *language-name*—This language will be displayed in the selection box on the login and portal pages. • *device*:*file*—Storage device on the system and the file name. The file name should include the directory location.

Command Default

English is the language.

Command Modes

Webvpn context configuration (config-webvpn-context)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Examples

The following example shows that the language to be used is Japanese:

```
Router (config)# webvpn context
 Router (config-webvpn-context)# language Japanese
```

The following example shows that the language (mylang) is to be customized from the file “lang.js,” which is in flash:

```
Router (config)# webvpn context
 Router (config-webvpn-context)# language customize mylang flash:lang.js
```

Related Commands

Command	Description
webvpn create template	Creates templates for multilanguage support for messages in an SSL VPN.

ldap attribute-map

To configure a dynamic Lightweight Directory Access Protocol (LDAP) attribute map, use the **ldap attribute-map** command in global configuration mode. To remove the attribute maps, use the **no** form of this command.

ldap attribute-map *map-name*

no ldap attribute-map *map-name*

Syntax Description

map-name	Name of the attribute map.

Command Default

Default mapping is applied.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

You can create LDAP attribute maps to map your existing user-defined LDAP attribute names and values to Cisco attribute names and values that are compatible. You can then bind these attribute maps to LDAP server configuration or remove them as required. The default map is displayed using the **show ldap attributes** command.

Examples

The following command shows how to create an unpopulated LDAP attribute map table named att_map_1:

```
Router(config)# ldap attribute-map att_map_1
```

Related Commands

Command	Description
attribute-map	Attaches an attribute map to a particular LDAP server.
map-type	Defines the mapping of a attribute in the LDAP server.
show ldap attribute	Displays information about default LDAP attribute mapping.

ldap search

To search a Lightweight Directory Access Protocol (LDAP) server, use the **ldap search** command in privileged EXEC mode.

ldap search *server-address port-number search-base scope-number search-filter* **ssl**

Syntax Description

server-address	The IP address of the server.
port-number	The remote TCP port. The range is from 0 to 65535.
search-base	The search base.
scope-number	The scope of the search. The range is from 0 to 2, which denotes to search from BASE, ONELEVEL, and SUBTREE.
search-filter	The filter for the search.
ssl	Specifies LDAP over Secure Socket Layer (SSL).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRB	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRB.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.

Examples

The following example shows how to search an LDAP server:

```
Router# ldap search 10.0.0.1 265 c 2 sea ssl
```

Related Commands

Command	Description
ldap server	Defines an LDAP server and enters LDAP server configuration mode.

ldap server

To define a Lightweight Directory Access Protocol (LDAP) server and enter LDAP server configuration mode, use the **ldap server** command in global configuration mode. To remove an LDAP server configuration, use the **no** form of this command.

ldap server *name*

no ldap server *name*

Syntax Description

name	Name of the LDAP server configuration.

Command Default

No LDAP server is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

You can define the following parameters in LDAP server configuration mode:

- IP address of the LDAP server
- Transport protocol to connect to the server
- Security protocol for peer-to-peer communication
- LDAP timers

Examples

The following example shows how to define an LDAP server named server1:

```
Router(config)# ldap server server1
```

Related Commands

Command	Description
ipv4 (ldap)	Creates an IPv4 address within an LDAP server address pool.
transport port (**ldap**)	Configures the transport protocol for establishing a connection with the LDAP server.

length (RITE)

To specify the length the captured portion of the packets being captured in IP traffic export capture mode, use the **length** command in RITE configuration mode. To return to the default condition of capturing entire packets, use the **no** form of this command.

length *bytes*

no length

Syntax Description

bytes	The length in bytes of the packet captured in IP traffic export capture mode. Acceptable values are 128, 256, and 512.

Command Default

When you do not use this command, the entire packet is captured.

Command Modes

RITE configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use this command to limit the length of the portion of the packets being captured in IP traffic export capture mode. The captured portion of the packets are limited to 128, 256, or 512 bytes. If you do not use the **length** command, entire packets are captured.

Examples

The following example shows the use of the **length** command in the configuration of IP traffic export capture mode profile “corp2”:

```
Router(config)# ip traffic-export profile corp2 mode_capture
Router(config-rite)# bidirectional
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# length 512
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp2 size 10000000
```

Related Commands

Command	Description
bidirectional	Enables incoming and outgoing IP traffic to be exported or captured across a monitored interface.
incoming	Configures filtering for incoming IP traffic export or IP traffic capture traffic.

Command	Description
ip traffic-export apply profile	Applies an IP traffic export or IP traffic capture profile to a specific interface.
ip traffic-export profile	Creates an IP traffic export or IP traffic capture profile on an ingress interface.
outgoing	Configures filtering for outgoing IP traffic export or IP traffic capture traffic.
traffic-export interface	Controls the operation of IP traffic capture mode.

lifetime (certificate server)

To specify the lifetime of the certification authority (CA) or a certificate, use the **lifetime** command in certificate server configuration mode. To return to the default lifetime values, use the **no** form of this command.

lifetime {**ca-certificate** | **certificate**} *days* [*hours* [*minutes*]]

no lifetime {**ca-certificate** | **certificate**}

Syntax Description

ca-certificate	Specifies that the lifetime applies to the CA certificate of the certificate server.
certificate	Specifies that the lifetime applies to the certificate of the certificate server. The maximum certificate lifetime is 1 month less than the expiration date of the CA certificate's lifetime.
days	An integer specifying the certificate lifetime in days. Valid values range from 0 to 7305.
hours	(Optional) An integer specifying the certificate lifetime in hours. Valid values range from 0 to 24.
minutes	(Optional) An integer specifying the certificate lifetime in minutes. Valid values range from 0 to 59. It is recommended that if you set the certificate lifetime in minutes, that the value be set to 3 minutes or greater. Setting the certificate lifetime to a value of less than 3 minutes will not allow certificate rollover to function.

Command Default

The default CA certificate lifetime is 1095 days, or 3 years.

The default certificate lifetime is 365 days, or 1 year.

Command Modes

Certificate server configuration (cs-server)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

After you enable a certificate server via the **crypto pki server** command, use the **lifetime** command if you wish to specify lifetime values other than the default values for the CA certificate and the certificate of the certificate server.

After the certificate generates its signed certificate, the lifetime cannot be changed. All certificates are valid when they are issued.

Examples

The following example shows how to set the lifetime value for the CA to 30 days:

```
Router(config)# ip http server
Router(config)# crypto pki server mycertserver
Router(cs-server)# lifetime ca certificate 30
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.

lifetime (IKE policy)

To specify the lifetime of an Internet Key Exchange (IKE) security association (SA), use the **lifetime** command in Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode. To reset the SA lifetime to the default value, use the **no** form of this command.

lifetime *seconds*

no lifetime

Syntax Description

seconds	Number of many seconds for each each SA should exist before expiring. Use an integer from 60 to 86,400 seconds, which is the default value.

Command Default

The default is 86,400 seconds (one day).

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to specify how long an IKE SA exists before expiring.

When IKE begins negotiations, the first thing it does is agree upon the security parameters for its own session. The agreed-upon parameters are then referenced by an SA at each peer. The SA is retained by each peer until the SA's lifetime expires. Before an SA expires, it can be reused by subsequent IKE negotiations, which can save time when setting up new IPSec SAs. Before an SA expires, it can be reused by subsequent IKE negotiations, which can save time when setting up new IPSec SAs. New IPSec SAs are negotiated before current IPSec SAs expire.

So, to save setup time for IPSec, configure a longer IKE SA lifetime. However, shorter lifetimes limit the exposure to attackers of this SA. The longer an SA is used, the more encrypted traffic can be gathered by an attacker and possibly used in an attack.

Note that when your local peer initiates an IKE negotiation between itself and a remote peer, an IKE policy can be selected only if the lifetime of the remote peer's policy is shorter than or equal to the lifetime of the local peer's policy. Then, if the lifetimes are not equal, the shorter lifetime will be selected. To restate this behavior: If the two peer's policies' lifetimes are not the same, the initiating peer's lifetime must be longer and the responding peer's lifetime must be shorter, and the shorter lifetime will be used.

Examples

The following example configures an IKE policy with a security association lifetime of 600 seconds (10 minutes), and all other parameters are set to the defaults:

```
crypto isakmp policy 15
 lifetime 600
 exit
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
group (IKE policy)	Specifies the Diffie-Hellman group identifier within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
show crypto isakmp policy	Displays the parameters for each IKE policy.

lifetime (IKEv2 profile)

To specify the lifetime for an Internet Key Exchange Version 2 (IKEv2) security association (SA), use the **lifetime** command in IKEv2 profile configuration mode. To reset the SA lifetime to the default value, use the **no** form of this command.

lifetime *seconds*

no lifetime

Syntax Description

seconds	The time that each IKE SA should exist before expiring. Use an integer from 60 to 86,400 seconds.

Command Default

The default is 86,400 seconds (one day).

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to specify the lifetime of an IKE SA. When IKE begins negotiations, IKE agrees on the security parameters for its session that are referenced by an SA at each peer. The SA is retained by each peer until the SA expires, and before an SA expires, it can be reused by subsequent IKE negotiations, which saves time when setting up new IKE SA. Although, SA with a shorter lifetime limits the exposure to attacks, to save time configure an IKE SA that has a longer lifetime. The longer an SA is used, the more encrypted traffic can be gathered by an attacker and possibly used in an attack.

Examples

The following example configures an IKEv2 profile with a security association lifetime of 600 seconds (10 minutes), and all other parameters are set to the defaults:

```
Router(config)# crypto ikev2 profile profile2
Router(config-ikev2-profile)# lifetime 600
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.
show crypto ikev2 profile	Displays the IKEv2 profile.

lifetime crl

To define the lifetime of the certificate revocation list (CRL) that is used by the certificate server, use the **lifetime crl** command in certificate server configuration mode. To return to the default value of 1 week, use the **no** form of this command.

lifetime crl *time*

no lifetime crl *time*

Syntax Description

time	Lifetime value, in hours, of the CRL. Maximum lifetime value is 336 hours (2 weeks). The default value is 168 hours (1 week).

Defaults

168 hours (1 week)

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

After you create a certificate server via the **crypto pki server** command, use the **lifetime crl** command if you want to specify a value other than the default value for the CRL. The lifetime value is added to the CRL when the CRL is created.

The CRL is written to the specified database location as *ca-label*.crl.

Examples

The following example shows how to set the lifetime value for the CRL to 24 hours:

```
Router(config)# ip http server
Router(config)# crypto pki server mycertserver
Router(cs-server)# lifetime crl 24
```

Related Commands

Command	Description
cdp-url	Specifies that CDP should be used in the certificates that are issued by the certificate server.
crypto pki server	Enables a Cisco IOS certificate server and enters PKI configuration mode.

lifetime enrollment-request

To specify how long an enrollment request should stay in the enrollment database, use the **lifetime enrollment-request** command in certificate server configuration mode. To return to the default value of 1 week, use the **no** form of this command.

lifetime enrollment-request *time*

no lifetime enrollment-request

Syntax Description

time	Lifetime value, in hours, of an enrollment request. The maximum lifetime value is 1000 hours. The default value is 168 hours (1 week).

Defaults

Lifetime value default is 168 hours.

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

After the certificate server receives an enrollment request, it can leave the request in pending, reject it, or grant it. The request is left in the Enrollment Request Database for the lifetime of the enrollment request until the client polls the certificate server for the result of the request.

Examples

The following example shows how to set the lifetime value for the enrollment request to 24 hours:

```
Router (config)# crypto pki server mycs
Router (cs-server)# lifetime enrollment-request 24
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server.
crypto pki server grant	Grants all or certain SCEP requests.
crypto pki server remove	Removes enrollment requests that are in the certificate server Enrollment Request Database.

list (LSP Attributes)

To display the contents of a label switched path (LSP) attribute list, use the **list** command in LSP Attributes configuration mode.

list

Syntax Description

This command has no arguments or keywords.

Command Default

Contents of an LSP attribute list is not displayed.

Command Modes

LSP Attributes configuration (config-lsp-attr)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command displays the contents of the LSP attribute list. You can display each of the following configurable LSP attributes using the **list** command: affinity, auto-bw, bandwidth, lockdown, priority, protection, and record-route.

Examples

The following example shows how to display the contents of an LSP attribute list identified with the string priority:

```
!
Router(config)# mpls traffic-eng lsp attributes priority
Router(config-lsp-attr)# priority 0 0
Router(config-lsp-attr)# list
 priority 0 0
Router(config-lsp-attr)#
```

Related Commands

Command	Description
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show mpls traffic-eng lsp attributes	Displays global LSP attribute lists.

list (WebVPN)

To list the currently configured access control list (ACL) entries sequentially, use the **list** command in webvpn acl configuration mode. This command has no **no** form.

list

Syntax Description

This command has no arguments or keywords.

Command Default

Currently configured ACL entries are not listed.

Command Modes

Webvpn acl configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Before using this command, you must have configured the web context and the **acl** command.

Examples

The following example shows that currently configured ACL entries are to be listed:

```
webvpn context context1
 acl acl1
  list
```

Related Commands

Command	Description
webvpn context	Configures the WebVPN context and enters SSL VPN configuration mode.
acl	Defines an ACL using a SSL VPN gateway at the Application Layer level.

li-view

To initialize a lawful intercept view, use the **li-view** command in global configuration mode.

li-view *li-password* **user** *username* **password** *password*

Syntax Description

li-password	Password for the lawful intercept view. This password is used by the system administrator or a level 15 privilege user who initialized the lawful intercept view to access and configure it. The password can contain any number of alphanumeric characters. **Note** The password is case sensitive.
user *username*	Specifies the user who can access the lawful intercept view.
password *password*	Provides the password for the specified user. The user must provide this password to access the lawful intercept view.

Defaults

A lawful intercept view cannot be accessed.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Like a command-line interface (CLI) view, a lawful intercept view restricts access to specified commands and configuration information. Specifically, a lawful intercept view allows a user to secure access to lawful intercept commands that are held within the TAP-MIB, which is a special set of Network Management Protocol (SNMP) commands that stores information about calls and users.

Commands available in lawful intercept view belong to one of the following categories:

- Lawful intercept commands that should not be made available to any other view or privilege level.
- CLI commands that are useful for lawful intercept users but do not need to be excluded from other views or privilege levels.

Note Only a system administrator or a level 15 privilege user can initialize a lawful intercept view.

Examples

The following example shows how to configure a lawful intercept view, add users to the view, and verify the users that were added to the view:

```
!Initialize the LI-View.
Router(config)# li-view lipass user li_admin password li_adminpass

00:19:25:%PARSER-6-LI_VIEW_INIT:LI-View initialized.
Router(config)# end

! Enter the LI-View; that is, check to see what commands are available within the view.
Router# enable view li-view
Password:

Router#
00:22:57:%PARSER-6-VIEW_SWITCH:successfully set to view 'li-view'.
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# parser view li-view
Router(config-view)# ?
View commands:
  commands  Configure commands for a view
  default   Set a command to its defaults
  exit      Exit from view configuration mode
  name      New LI-View name      ===This option only resides in LI View.
  no        Negate a command or set its defaults
  password  Set a password associated with CLI views

Router(config-view)#

! NOTE:LI View configurations are never shown as part of 'running-configuration'.

! Configure LI Users.
Router(config)# username lawful-intercept li-user1 password li-user1pass
Router(config)# username lawful-intercept li-user2 password li-user2pass

! Displaying LI User information.
Router# show users lawful-intercept

li_admin
li-user1
li-user2
Router#
```

Related Commands

Command	Description
show users	Displays information about the active lines on the router.
username	Establishes a username-based authentication system.

load-balance (server-group)

To enable RADIUS server load balancing for a named RADIUS server group, use the **load-balance** command in server group configuration mode. To disable named RADIUS server load balancing, use the **no** form of this command.

load-balance method least-outstanding [**batch-size** *number*] [**ignore-preferred-server**]

no load-balance

Syntax Description

method least-outstanding	Enables least outstanding mode for load balancing.
batch-size	(Optional) The number of transactions to be assigned per batch.
number	(Optional) The number of transactions in a batch. • The default is 25. • The range is 1–2147483647. **Note** Batch size may impact throughput and CPU load. It is recommended that the default batch size, 25, be used because it is optimal for high throughput, without adversely impacting CPU load.
ignore-preferred-server	(Optional) Indicates if a transaction associated with a single authentication, authorization, and accounting (AAA) session should attempt to use the same server or not. • If set, preferred server setting will not be used. • Default is to use the preferred server.

Command Defaults

If this command is not configured, named RADIUS server load balancing will not occur.

Command Modes

Server group configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Examples

The following example shows load balancing enabled for a named RADIUS server group. It is shown in three parts: the current configuration of RADIUS command output, debug output, and AAA server status information.

Server Configuration and Enabling Load Balancing for Named RADIUS Server Group Example

The following shows the relevant RADIUS configuration:

```
Router# show running-config
```

```
.
.
.
aaa group server radius server-group1
 server 192.0.2.238 auth-port 2095 acct-port 2096
 server 192.0.2.238 auth-port 2015 acct-port 2016
 load-balance method least-outstanding batch-size 5
!
aaa authentication ppp default group server-group1
aaa accounting network default start-stop group server-group1
.
.
.
```

The lines in the current configuration of RADIUS command output above are defined as follows:

- The **aaa group server radius** command shows the configuration of a server group with two member servers.
- The **load-balance** command enables load balancing for the global RADIUS server groups with the batch size specified.
- The **aaa authentication ppp** command authenticates all PPP users using RADIUS.
- The **aaa accounting** command enables the sending of all accounting requests to the AAA server after the client is authenticated and after the disconnect using the start-stop keyword.

Debug Output for Named RADIUS Server Group Example

The debug output below shows the selection of a preferred server and the processing of requests for the configuration above.

```
Router#
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Server[0] load:0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Selected Server[0] with load 0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002E):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002E):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002F):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002F):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(00000030):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
```

```
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(00000030):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000031):No preferred server available.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Server[0] load:5
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Selected Server[1] with load 0
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000031):Server (192.0.2.238:2015,2016) now
being used as preferred server
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000032):No preferred server available.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
.
.
.
```

Server Status Information for Named RADIUS Server Group Example

The output below shows the AAA server status for the named RADIUS server group configuration example.

```
Router# show aaa servers

RADIUS:id 8, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
     State:current UP, duration 3781s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Elapsed time since counters last cleared:0m

RADIUS:id 9, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
     State:current UP, duration 3781s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Elapsed time since counters last cleared:0m
Router#
```

The output shows the status of two RADIUS servers. Both servers are alive, and no requests have been processed since the counters were cleared 0 minutes ago.

Related Commands

Command	Description
debug aaa sg-server selection	Shows why the RADIUS and TACACS+ server group system in a router is selecting a particular server.
debug aaa test	Shows when the idle timer or dead timer has expired for RADIUS load balancing.
radius-server host	Enables RADIUS automated testing for load balancing.
radius-server load-balance	Enables RADIUS server load balancing for the global RADIUS server group.
test aaa group	Tests RADIUS load balancing server response manually.

load classification

To load a traffic classification definition file (TCDF) for a Flexible Packet Matching (FPM) configuration, use the **load classification** command in global configuration mode. To unload all TCDFs from a specified location or a single TCDF, use the **no** form of this command.

load classification *location*:*filename*

no load classification *location*:*filename*

Syntax Description

location:*filename*	Location of the TCDF that is to be loaded onto the router. When used with the **no** form of this command, all TCDFs loaded from the specified filename will be unloaded. **Note** The location must be local to the routing device.

Command Default

No TCDF is loaded onto the router.

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

A TCDF is an Extensible Markup Language (XML) file that you create in a text file or using an XML editor. FPM uses a TCDF to define classes of traffic and to specify actions to apply to the traffic classes for the purpose of blocking attacks on the network. Traffic classification behavior defined in a TCDF is identical to that configured using the command-line interface (CLI).

Use the **load classification** command to load the TCDF onto the routing device. The location to which you load the file must be local to the device. After the TCDF is loaded, you can use service policy CLI commands to attach the TCDF policies to a specific interface or interfaces. TCDP classes and policies, which are loaded, display as normal policies and classes when you issue a **show** command.

The TCDF requires that a relevant protocol header description file (PHDF) is already loaded onto the system through the use of the **load protocol** command. Standard PHDFs are provided with the FPM feature.

Examples

The following example shows how to create a TCDF for slammer packets (UDP 1434) for an FPM XML configuration. The match criteria defined within the **class** element is for slammer packets with an IP length not to exceed 404 (0x194) bytes, UDP port 1434 (0x59A), and pattern 0x4011010 at 224 bytes from start of the IP header. The policy “fpm-udp-policy” is defined with the action to drop slammer packets.

```
<?xml version="1.0" encoding="UTF-8"?>
<tcdf>
```

```
    <class name="ip-udp" type="stack">
       <match>
          <eq field="ip.protocol" value="0x11" next="udp"></eq>
       </match>
    </class>

    <class name="slammer" type="access-control" match="all">
       <match>
          <eq field="udp.dest-port" value="0x59A"></eq>
          <eq field="ip.length" value="0x194"></eq>
          <eq start="l3-start" offset="224" size="4" value="0x00401010"></eq>
       </match>
    </class>

    <policy type="access-control" name="fpm-udp-policy">
       <class name="slammer"></class>
       <action>drop</action>
    </policy>
</tcdf>
```

The following example shows how to load relevant PHDFs, load the TCDF file sql-slammer.tcdf, and attach the TCDF-defined policy to the interface Ethernet 0/1:

```
enable
configure terminal

load protocol localdisk1:ip.phdf
load protocol localdisk1:tcp.phdf
load protocol localdisk1:udp.phdf

load classification localdisk1:sql-slammer.tcdf

policy-map type access-control my-policy-1
class ip-udp
service-policy fpm-udp-policy

interface Ethernet 0/1
 service-policy type access control input my-policy-1
 end
```

The following CLI output is associated with the TCDF described in the example:

```
Router# show class-map type stack
.
.
.
class-map type stack match-all ip-udp
   match field IP protocol eq 0x11 next UDP
.
.
.
Router# show class-map type access-control
.
.
.

class-map type access-control match-all slammer
   match field UDP dest-port eq 0x59A
   match field IP length eq 0x194
   match start l3-start offset 224 size 4 eq 0x4011010
.
.
.
```

```
Router show policy-map my-policy-1
.
.
.

policy-map type access-control my-policy-1
  class slammer
    drop
.
.
.
```

Related Commands

Command	Description
load protocol	Loads a protocol header description file (PHDF) onto a router.

local-address

To limit the scope of an Internet Security Association and Key Management Protocol (ISAKMP) profile or an ISAKMP keyring configuration to a local termination address or interface, use the **local-address** command in ISAKMP profile configuration and keyring configuration modes. To remove the local address or interface, use the **no** form of this command.

local-address {*interface-name* | *ip-address* [*vrf-tag*]}

no local-address {*interface-name* | *ip-address* [*vrf-tag*]}

Syntax Description

interface-name	Name of the local interface.
ip-address	Local termination address.
vrf-tag	(Optional) Scope of the IP address will be limited to the VRF instance.

Defaults

If this command is not configured, the ISAKMP profile or ISAKMP keyring is available to all local addresses.

Command Modes

ISAKMP profile configuration
Keyring configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Examples

The following example shows that the scope of the ISAKMP profile is limited to interface serial2/0:

```
crypto isakmp profile profile1
  keyring keyring1
  match identity address 10.0.0.0 255.0.0.0
  local-address serial2/0
```

The following example shows that the scope of the ISAKMP keyring is limited only to interface serial2/0:

```
crypto keyring
  local-address serial2/0
  pre-shared-key address 10.0.0.1
```

The following example shows that the scope of the ISAKMP keyring is limited only to IP address 10.0.0.2:

```
crypto keyring keyring1
  local-address 10.0.0.2
  pre-shared-key address 10.0.0.2 key
```

The following example shows that the scope of an ISAKMP keyring is limited to IP address 10.34.35.36 and that the scope is limited to VRF examplevrf1:

```
ip vrf examplevrf1
  rd 12:3456
crypto keyring ring1
  local-address 10.34.35.36 examplevrf1
interface ethernet2/0
  ip vrf forwarding examplevrf1
  ip address 10.34.35.36 255.255.0.0
```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile and audits IPSec user sessions.
crypto keyring	Defines a keyring and enters keyring configuration mode.

local-port (WebVPN)

To remap (forward) an application port number in a port forwarding list, use the **local-port** command in webvpn port-forward list configuration mode. To remove the application port mapping from the forwarding list, use the **no** form of this command.

local-port *number* **remote-server** *name* **remote-port** *number* **description** *text-string*

no local-port *number*

Syntax Description

number	Configures the port number to which the local application is mapped. Valid values are 1 to 65535.
remote-server *name*	Identifies the remote server. An IPv4 address or fully qualified domain name is entered.
remote-port *number*	Specifies the well-known port number of the application, for which port-forwarding is to be configured. Valid values are 1 to 65535.
description *text-string*	Configures a description for this entry in the port-forwarding list. The text string is displayed on the end-user applet window. A text string up to 64 characters in length is entered.

Command Default

An application port number is not remapped.

Command Modes

Webvpn port-forward list configuration (config-webvpn-port-fwd)

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The **local-port** command is configured to add an entry to the port-forwarding list. The forward list is created with the **port-forward** command in webvpn context configuration mode. The remote port number is the well-known port to which the application listens. The local port number is the entry configured in the port forwarding list. A local port number can be configured only once in a given port-forwarding list.

Examples

The following example configures port forwarding for well-known e-mail application port numbers:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# port-forward EMAIL
Router(config-webvpn-port-fwd)# local-port 30016 remote-server mail.company.com
remote-port 110 description POP3
Router(config-webvpn-port-fwd)# local-port 30017 remote-server mail.company.com
remote-port 25 description SMTP
Router(config-webvpn-port-fwd)# local-port 30018 remote-server mail.company.com
remote-port 143 description IMAP
```

Related Commands

Command	Description
port-forward	Enters webvpn port-forward list configuration mode to configure a port-forwarding list.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

local priority

To set the local key server priority, use the **local priority** command in GDOI redundancy configuration mode. To remove the local key server priority that was set, use the **no** form of this command.

local priority *number*

no local priority *number*

Syntax Description

number	Priority number of the local server. Value = 1 through 255.

Command Default

If the local priority is not set by this command, the local priority defaults to 1.

Command Modes

GDOI redundancy configuration (gdoi-coop-ks-config)

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 Aggregation Services Series Routers

Usage Guidelines

Configure the priority to determine the order of preference of the key servers (the higher priority device becomes the primary key server). If the priority of two devices is the same, the IP address is used to set the priority. The higher the IP address, the higher the priority.

Note If the **no local priority** option is configured, the default value of 1 is set for that key server.

Examples

The following example shows that the key server 10.1.1.1 has the highest priority and, therefore, becomes the primary key server:

```
address ipv4 10.1.1.1
redundancy
 local priority 10
 peer address ipv4 10.41.2.5
 peer address ipv4 10.33.5.6
address ipv4 10.41.2.5
redundancy
 peer address ipv4 10.1.1.1
 peer address ipv4 10.33.5.6
address ipv4 10.33.5.6
redundancy
 local priority 5
 peer address ipv4 10.41.2.5
 peer address ipv4 10.1.1.1
```

Related Commands

Command	Description
address ipv4	Sets the source address, which is used as the source for packets originated by the local key server.
peer address ipv4	Configures a GDOI redundant peer key server.
redundancy	Enters GDOI redundancy configuration mode and allows for peer key server redundancy.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

lockdown (LSP Attributes)

To disable reoptimization of the label switched path (LSP), use the **lockdown** command in LSP Attributes configuration mode. To reenable reoptimization, use the **no** form of this command.

lockdown

no lockdown

Syntax Description

This command has no arguments or keywords.

Command Default

Reoptimization of the LSP is enabled.

Command Modes

LSP Attributes configuration (config-lsp-attr)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to set up in an LSP attribute list the disabling of reoptimization of an LSP triggered by a timer, or the issuance of the **mpls traffic-eng reoptimize** command, or a configuration change that requires the resignalling of an LSP.

To associate the LSP lockdown attribute and the LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where *string* is the identifier for the specific LSP attribute list.

Examples

The following example shows how to configure disabling of reoptimization in an LSP attribute list:

```
Configure terminal
!
mpls traffic-eng lsp attributes 4
 bandwidth 1000
 priority 1 1
 lockdown
 end
```

Related Commands

Command	Description
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show mpls traffic-eng lsp attributes	Displays global LSP attribute lists.

log (policy-map)

To generate a log of messages, use the **log** command in policy-map configuration mode. To disable the log, use the **no** form of this command.

log

no log

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Policy-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced in Cisco IOS Release 12.4(6)T.
12.4(20)T	This command was modified in Cisco IOS Release 12.4(20)T. This command can now be used after entering the **policy-map type inspect smtp**.

Usage Guidelines

You can use this command only after entering the following commands:

- **policy-map type inspect http**
- **policy-map type inspect imap**
- **policy-map type inspect smtp**

Examples

The following example generates a log of messages:

```
policy-map type inspect http mypolicy
 log
```

Related Commands

Command	Description
policy-map type inspect http	Creates a Layer 7 HTTP policy map.
policy-map type inspect imap	Creates a Layer 7 IMAP policy map.
policy-map type inspect smtp	Create a Layer 7 SMTP policy map

log (parameter-map type)

To log the firewall activity for an inspect parameter map, use the **log** command in parameter-map type inspect configuration mode.

log {**dropped-packets** {**disable** | **enable**} | **summary** [**flows** *number*] [**time-interval** *seconds*]}

Syntax Description

dropped-packets	Logs the packets dropped by the firewall.
disable | enable	Disables or enables logging the dropped packets.
summary	Turns on the summary of the packets dropped during the firewall activity for interzone and intrazone traffic.
flows *number*	(Optional) Specifies the number of flows for which the summary logs must be printed. The default flow is 16.
time-interval *seconds*	(Optional) Specifies the time interval, in seconds. which the summary logs must be printed. The default is 60.

Command Default

The firewall activity is not captured.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

Use this command to log the firewall activity as follows:

- Time interval for the summary logs
- Display the protocol information in the summary logs
- Enable summary logs for the specified flows

If the flow is specified as zero as **log summary flow 0**, the log activity is turned off and summary logs are not printed until the flow count is greater than zero.

To display the summary logs, use the **show policy-firewall summary-log** and **clear policy-firewall summary-log** to clear the summary logs.

Examples

The following examples show how to configure the summary logs in two scenarios.

In the following example, the summary logs are printed for 40 flows every 2 minutes:

```
Router(config)# parameter-map type inspect global
Router(config-profile)# log summary flows 40 time-interval 120
```

In the following example, the summary logs are printed for 30 flows at the default time interval of 1 minute:

```
Router(config)# parameter-map type inspect global
```

```
Router(config-profile)# log summary flows 30
```

In the above example, the flow is not configured. Hence, the summary logs are printed by default for 16 flows every 30 seconds:

```
Router(config)# parameter-map type inspect global
Router(config-profile)# log summary time-interval 30
```

Related Commands

Command	Description
clear policy-firewall	Clears the information collected by the firewall.
parameter-map type inspect	Defines an inspect type parameter map.
show policy-firewall summary-log	Displays the summary log of the firewall.

log (type access-control)

To generate log messages for a predefined traffic class, use the **log** command in policy-map class configuration mode. To disable the log, use the **no** form of this command.

log [**all**]

no log [**all**]

Syntax Description

all	(Optional) Logs the entire stream of discarded packets belonging to the traffic class.

Command Default

Log messages are disabled.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

If the **log** command is specified with the **all** keyword, then this command can only be used with a predefined session-based Flexible Packet Matching (FPM) traffic class that was created with the **class-map type access-control** command.

The **log all** command is used when configuring a policy map that can be attached to one or more interfaces to specify a service policy that is created with the **policy-map type access-control** command.

Examples

The following example shows how to configure a class map and policy map to specify the protocol stack class, the match criteria and action to take, and a combination of classes using session-based (flow-based) and nonsession-based actions. The **log** command's **all** keyword is associated with the action to be taken on the policy.

```
Router(config)# class-map type access-control match-all my-HTTP
Router(config-cm)# match field tcp destport eq 8080
Router(config-cm)# match start tcp payload-start offset 20 size 10 regex "GET"

Router(config)# class-map type access-control match-all my-FTP
Router(config-cmap)# match field tcp destport eq 21

Router(config)# class-map type access-control match all class1
Router(config-cmap)# match class my-HTTP session
Router(config-cmap)# match start tcp payload-start offset 40 size 20 regex "abc.*def"

Router(config)# policy-map type access-control my_http_policy
Router(config-pmap)# class class1
Router(config-pmap-c)# log all

Router(config)# interface gigabitEthernet 0/1
```

```
Router(config-if)# service-policy type access-control input my_http_policy
```

Related Commands

Command	Description
class	Specifies the name of a predefined traffic class, which was configured with the **class-map** command. The **class** command also classifies traffic to the traffic policy and enters policy-map class configuration mode.
class-map type access-control	Creates a class map to be used for matching packets to a specified class and enters class map configuration mode for determining the exact pattern to look for in the protocol stack of interest.
drop	Configures a traffic class to discard packets belonging to a specific class.
match class session	Configures match criteria for a class map used to identify a session (flow) containing packets of interest, which is then applied to all packets transmitted during the session.
policy-map type access-control	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy, and enters policy-map configuration mode.
show class-map	Displays all class maps and their matching criteria.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.

logging dmvpn

To display Dynamic Multipoint VPN (DMVPN)-specific system logging information, use the **logging dmvpn** command in global configuration mode. To turn off logging, use the **no** form of this command.

logging dmvpn [**rate-limit** *rate*]

no logging dmvpn [**rate-limit** *rate*]

Syntax Description

rate-limit *rate*	(Optional) Specifies the number of DMVPN syslog messages generated per minute. The range is from 1 to 10000. • The default rate is to generate 600 messages per minute.

Command Default

DMVPN system logging messages are not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(9)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.0(1)M	This command was modified. The *rate* argument was modified to specify the number of DMVPN syslog messages per minute.

Usage Guidelines

Use the **logging dmvpn rate-limit** *rate* command to specify the rate at which the DMVPN-specific syslog messages are displayed. In Cisco IOS Release 12.4(24)T and earlier releases, the *rate* argument specifies the minimum interval, in seconds, between two DMVPN syslog messages, with a range of 0 to 3600, and a default value of 60.

In Cisco IOS Release 15.0(1)M and later releases, the *rate* argument specifies the number of DMVPN syslog messages per minute. If you have upgraded to Release Cisco IOS 15.0(1)M or later releases, you must reconfigure the DMVPN rate limit settings.

Examples

The following example shows how to configure the router to display five DMVPN-specific syslog messages per minute:

```
Router> enable
Router# configure terminal
Router(config)# logging dmvpn rate-limit 5
```

The following example shows a sample system log with DMVPN messages:

```
%DMVPN-7-CRYPTO_SS: Tunnel101-192.0.2.1 socket is UP
%DMVPN-5-NHRP_NHS: Tunnel101 192.0.2.251 is UP
```

```
%DMVPN-5-NHRP_CACHE: Client 192.0.2.2 on Tunnel1 Registered.
%DMVPN-5-NHRP_CACHE: Client 192.0.2.2 on Tunnel101 came UP.
%DMVPN-3-NHRP_ERROR: Registration Request failed for 192.0.2.251 on Tunnel101
```

Related Commands

Command	Description
debug dmvpn	Debugs DMVPN sessions.

logging enabled

To enable syslog messages, use the **logging enabled** command in parameter-map-type consent configuration mode.

logging enabled

Syntax Description

This command has no arguments or keywords.

Command Default

Logging messages are not enabled.

Command Modes

Parameter-map-type consent (config-profile)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

After the **logging enabled** command is entered, a log entry (a syslog), including the client's IP address and the time, is created everytime a response is received for the consent web page.

Examples

The following example shows how to define the consent-specific parameter map "consent_parameter_map" and a default consent parameter map. In both parameter maps, logging is enabled.

```
parameter-map type consent consent_parameter_map
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity consent_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
parameter-map type consent default
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity test_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
```

logging ip access-list cache (global configuration)

To configure the Optimized ACL Logging (OAL) parameters, use the **logging ip access-list cache** command in global configuration mode. To return to the default settings, use the **no** form of this command.

logging ip access-list cache {**entries** *entries* | {**interval** *seconds* | **rate-limit** *pps* | **threshold** *packets*}

no logging ip access-list cache [**entries** | **interval** | **rate-limit** | **threshold**]

Syntax Description

entries *entries*	Specifies the maximum number of log entries that are cached in the software; valid values are from 0 to 1048576 entries.
interval *seconds*	Specifies the maximum time interval before an entry is sent to syslog; valid values are from 5 to 86400 seconds.
rate-limit *pps*	Specifies the number of packets that are logged per second in the software; valid values are from 10 to 1000000 pps.
threshold *packets*	Specifies the number of packet matches before an entry is sent to syslog; valid values are from 1 to 1000000 packets.

Defaults

The defaults are as follows:

- *entries*—**8000** entries.
- *seconds*—**300** seconds (5 minutes).
- **rate-limit** *pps*—**0** (rate limiting is off) and all packets are logged.
- **threshold** *packets*—**0** (rate limiting is off) and the system log is not triggered by the number of packet matches.

Command Modes

Global configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720 only.

OAL is supported on IPv4 unicast traffic only.

You cannot configure OAL and VACL capture on the same chassis. OAL and VACL capture are incompatible. With OAL configured, use SPAN to capture traffic.

If the entry is inactive for the duration that is specified in the **update-interval** *seconds* command, the entry is removed from the cache.

If you enter the **no logging ip access-list cache** command without keywords, all the parameters are returned to the default values.

You must set ICMP unreachable rate limiting to 0 if the OAL is configured to log denied packets.

Examples

This example shows how to specify the maximum number of log entries that are cached in the software:

```
Router(config)# logging ip access-list cache entries 200
```

This example shows how to specify the maximum time interval before an entry is sent to the system log:

```
Router(config)# logging ip access-list cache interval 350
```

This example shows how to specify the number of packets that are logged per second in the software:

```
Router(config)# logging ip access-list cache rate-limit 100
```

This example shows how to specify the number of packet matches before an entry is sent to the system log:

```
Router(config)# logging ip access-list cache threshold 125
```

Related Commands

Command	Description
clear logging ip access-list cache	Clears all the entries from the OAL cache and sends them to the syslog.
logging ip access-list cache (interface configuration)	Enables an OAL-logging cache on an interface that is based on direction.
show logging ip access-list	Displays information about the logging IP access list.
update-interval *seconds*	Removes entries from the cache that are inactive for the duration that is specified in the command.

logging ip access-list cache (interface configuration)

To enable an Optimized ACL Logging (OAL)-logging cache on an interface that is based on direction, use the **logging ip access-list cache** command in interface configuration mode. To disable OAL, use the **no** form of this command.

logging ip access-list cache [**in** | **out**]

no logging ip access-list cache

Syntax Description

in	(Optional) Enables OAL on ingress packets.
out	(Optional) Enables OAL on egress packets.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720 only.

This command is supported on traffic that matches the **log** keyword in the applied ACL. You must set ICMP unreachable rate limiting to 0 if the OAL is configured to log denied packets.

On systems that are configured with a PFC3A, support for the egress direction on tunnel interfaces is not supported.

OAL is supported on IPv4 unicast traffic only.

You cannot configure OAL and VACL capture on the same chassis. OAL and VACL capture are incompatible. With OAL configured, use SPAN to capture traffic.

If the entry is inactive for the duration that is specified in the **update-interval** *seconds* command, the entry is removed from the cache.

If you enter the **no logging ip access-list cache** command without keywords, all the parameters are returned to the default values.

Examples

This example shows how to enable OAL on ingress packets:

```
Router(config-if)# logging ip access-list cache in
```

This example shows how to enable OAL on egress packets:

```
Router(config-if)# logging ip access-list cache out
```

Related Commands

Command	Description
clear logging ip access-list cache	Clears all the entries from the OAL cache and sends them to the syslog.
logging ip access-list cache (global configuration)	Configures the OAL parameters.
show logging ip access-list	Displays information about the logging IP access list.
update-interval *seconds*	Removes entries from the cache that are inactive for the duration that is specified in the command.

login authentication

To enable authentication, authorization, and accounting (AAA) authentication for logins, use the **login authentication** command in line configuration mode. To return to the default specified by the **aaa authentication login** command, use the **no** form of this command.

login authentication {**default** | *list-name*}

no login authentication {**default** | *list-name*}

Syntax Description

default	Uses the default list created with the **aaa authentication login** command.
list-name	Uses the indicated list created with the **aaa authentication login** command.

Defaults

Uses the default set with **aaa authentication login**.

Command Modes

Line configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is a per-line command used with AAA that specifies the name of a list of AAA authentication methods to try at login. If no list is specified, the default list is used (whether or not it is specified in the command line).

Caution If you use a *list-name* value that was not configured with the **aaa authentication login** command, you will disable login on this line.

Entering the **no** version of **login authentication** has the same effect as entering the command with the **default** keyword.

Before issuing this command, create a list of authentication processes by using the global configuration **aaa authentication login** command.

Examples

The following example specifies that the default AAA authentication is to be used on line 4:

```
line 4
 login authentication default
```

The following example specifies that the AAA authentication list called *list1* is to be used on line 7:

```
line 7
 login authentication list1
```

Related Commands

Command	Description
aaa authentication login	Sets AAA authentication at login.

login block-for

To configure your Cisco IOS device for login parameters that help provide denial-of-service (DoS) detection, use the **login block-for** command in global configuration mode. To disable the specified login parameters and return to the default functionality, use the **no** form of this command.

login block-for *seconds* **attempts** *tries* **within** *seconds*

no login block-for

Syntax Description

seconds	Duration of time in which login attempts are denied (also known as a quiet period) by the Cisco IOS device. Valid values range from 1 to 65535 (18 hours) seconds.
attempts *tries*	Maximum number of failed login attempts that triggers the quiet period. Valid values range from 1 to 65535 tries.
within *seconds*	Duration of time in which the allowed number of failed login attempts must be made before the quiet period is triggered. Valid values range from 1 to 65535 (18 hours) seconds.

Defaults

No login parameters are defined.

A quiet period is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25).
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

If the specified number of connection attempts (via the **attempts** *tries* option) fail within a specified time (via the **within** *seconds* option), the Cisco IOS device will not accept any additional login attempts for a specified period of time (via the *seconds* argument).

All login parameters are disabled by default. You must issue the **login block-for** command, which enables default login functionality, before using any other login commands. After the **login block-for** command is enabled, the following defaults are enforced:

- A default login delay of 1 second

- All login attempts made via Telnet and secure shell (SSH) are denied during the quiet period; that is, no access control lists (ACLs) are exempt from the login period until the **login quiet-mode access-class** command is issued. If this command is not configured, then the default ACL **sl_def_acl** is created on the router. This ACL is hidden in the running configuration. Use the **show access-list sl_def_acl** to view the parameters for the default ACL.

  For example:

```
Router#show access-lists sl_def_acl

Extended IP access list sl_def_acl
    10 deny tcp any any eq telnet
    20 deny tcp any any eq www
    30 deny tcp any any eq 22
    40 permit ip any any
```

System Logging Messages

The following logging message is generated after the router switches to quiet mode:

```
00:04:07:%SEC_LOGIN-1-QUIET_MODE_ON:Still timeleft for watching failures is 158 seconds,
[user:sfd] [Source:10.4.2.11] [localport:23] [Reason:Invalid login], [ACL:22] at 16:17:23
UTC Wed Feb 26 2003
```

The following logging message is generated after the router switches from quiet mode back to normal mode:

```
00:09:07:%SEC_LOGIN-5-QUIET_MODE_OFF:Quiet Mode is OFF, because block period timed out at
16:22:23 UTC Wed Feb 26 2003
```

Examples

The following example shows how to configure your router to block all login requests for 100 seconds if 15 failed login attempts are exceeded within 100 seconds. Thereafter, the **show login** command is issued to verify the login settings.

```
Router(config)# login block-for 100 attempts 15 within 100
Router(config)# exit
Router# show login

A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.

Router enabled to watch for login Attacks.
If more than 15 login failures occur in 100 seconds or less, logins will be disabled for
100 seconds.

Router presently in Watch-Mode, will remain in Watch-Mode for 95 seconds.
Present login failure count 5
```

The following example shows how to disable login parameters. Thereafter, the **show login** command is issued to verify that login parameters are no longer configured.

```
Router(config)# no login block-for
Router(config)# exit
```

```
Router# show login

No login delay has been applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps

Router NOT enabled to watch for login Attacks
```

Related Commands

Command	Description
login delay	Configures a uniform delay between successive login attempts.
login quiet-mode access-class	Specifies an ACL that is to be applied to the router when it switches to quiet mode.
show login	Displays login parameters.

login delay

To configure a uniform delay between successive login attempts, use the **login delay** command in global configuration mode. To return to the default functionality (which is a 1 second delay), use the **no** form of this command.

login delay *seconds*

no login delay

Syntax Description

seconds	Number of seconds between each login attempt. Valid values range from 1 to 10 seconds.

Defaults

If this command is not enabled, a login delay of 1 second is automatically enforced.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

A Cisco IOS device can accept connections (such as Telnet, secure shell (SSH), and HTTP) as fast as they can be processed. The **login delay** command introduces a uniform delay between successive login attempts. (The delay occurs for all login attempts—failed or successful attempts.) Thus, user users can better secure their Cisco IOS device from dictionary attacks, which are an attempt to gain username and password access to your device.

Although the **login delay** command allows users to configure a specific a delay, a uniform delay of 1 second is enabled if the **auto secure** command is issued. After the **auto secure** command is enabled, the autosecure dialog prompts users for login parameters; if login parameters have already been configured, the autosecure dialog will retain the specified values.

Examples

The following example shows how to configure your router to issue a delay of 10 seconds between each successive login attempt:

```
Router(config)# login delay 10
```

Related Commands

Command	Description
auto secure	Secures the management and forwarding planes of the router.
login block-for	Configures your Cisco IOS device for login parameters that help provide DoS detection.
show login	Displays login parameters.

login-message

To configure a login message for the text box on the user login page, use the **login-message** command in webvpn context configuration mode. To reconfigure the SSL VPN context configuration to display the default message, use the **no** form of this command.

login-message [*message-string*]

no login-message [*message-string*]

Syntax Description

message-string	(Optional) Login message string up to 255 characters in length. The string value may contain 7-bit ASCII values, HTML tags, and escape sequences.

Defaults

The following message is displayed if this command is not configured or if the **no** form is entered:

"Please enter your username and password"

Command Modes

Webvpn context configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The optional form of this command is used to change or enter a login message. A text string up to 255 characters in length can be entered. The **no** form of this command is entered to configure the default message to be displayed. When the **login-message** command is entered without the optional text string, no login message is displayed.

Examples

The following example changes the default login message to "Please enter your login credentials":

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# login-message "Please enter your login credentials"
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

login quiet-mode access-class

To specify an access control list (ACL) that is to be applied to the router when the router switches to quiet mode, use the **login quiet-mode access-class** command in global configuration mode. To remove this ACL and allow the router to deny all login attempts, use the **no** form of this command.

login quiet-mode access-class {*acl-name* | *acl-number*}

no login quiet-mode access-class {*acl-name* | *acl-number*}

Syntax Description

acl-name	Named ACL that is to be enforced during quiet mode.
acl-number	Numbered (standard or extended) ACL that is to be enforced during quiet mode.

Defaults

All login attempts via Telnet, secure shell (SSH), and HTTP are denied.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Before using this command, you must issue the **login block-for** command, which allows you to specify the necessary parameters to enable a quiet period.

- Use the **login quiet-mode access-class** command to selectively allow hosts on the basis of a specified ACL. You may use this command to grant an active client or list of clients an infinite number of failed attempts that are not counted by the router; that is, the active clients are placed on a “safe list” that allows them access to the router despite a quiet period. If this command is not configured, then the default ACL **sl_def_acl** is created on the router. This ACL is hidden in the running configuration. Use the **show access-list sl_def_acl** to view the parameters for the default ACL.

  For example:

```
Router#show access-lists sl_def_acl

Extended IP access list sl_def_acl
    10 deny tcp any any eq telnet
    20 deny tcp any any eq www
    30 deny tcp any any eq 22
    40 permit ip any any
```

System Logging Messages

The following logging message is generated after the router switches to quiet mode:

```
00:04:07:%SEC_LOGIN-1-QUIET_MODE_ON:Still timeleft for watching failures is 158 seconds,
[user:sfd] [Source:10.4.2.11] [localport:23] [Reason:Invalid login], [ACL:22] at 16:17:23
UTC Wed Feb 26 2003
```

The following logging message is generated after the router switches from quiet mode back to normal mode:

```
00:09:07:%SEC_LOGIN-5-QUIET_MODE_OFF:Quiet Mode is OFF, because block period timed out at
16:22:23 UTC Wed Feb 26 2003
```

Examples

The following example shows how to configure your router to accept hosts only from the ACL “myacl” during the next quiet period:

```
Router(config)# login quiet-mode access-class myacl
```

Related Commands

Command	Description
login block-for	Configures your Cisco IOS device for login parameters that help provide DoS detection.
show login	Displays login parameters.

login-photo

To set the photo parameters on a Secure Socket Layer Virtual Private Network (SSL VPN) login page, use the **login-photo** command in web vpn context configuration mode. To display the login page with no photo but with a message that spans the message and the photo columns, use the **no** form of this command.

login-photo [**file** *file-name* | **none**]

no login-photo

Syntax Description

file *file-name*	Points to a file to be displayed on the login page. The *file-name* argument can be **jpeg**, **bitmap**, or **gif**. However, gif files are recommended.
none	No photo appears on the login page.

Command Default

No photo appears, and the message spans the two columns (message and photo columns).

Command Modes

Webvpn context configuration (config-webvpn-context)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

To display no photo, use the **login-photo none** option. To display no photo and have the message span both columns (message column and photo column), use the **no login-photo** option.

The best resolution for login photos is 179 x 152 pixels.

Examples

The following example shows that no photo is displayed:

```
Router (config)# webvpn context
Router (config-webvpn-context)# login-photo none
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

logo

To configure a custom logo to be displayed on the login and portal pages of an SSL VPN, use the **logo** command in SSLVPN configuration mode. To configure the Cisco logo to be displayed, use the **no** form of this command.

logo [**file** *filename* | **none**]

no logo [**file** *filename* | **none**]

Syntax Description

file *filename*	(Optional) Specifies the location of an image file. A gif, jpg, or png file can be specified. The file can be up to 100 KB in size. The name of the file can be up 255 characters in length.
none	(Optional) No logo is displayed.

Defaults

The Cisco logo is displayed if the **no** form of this command is not configured or if the **no** form is entered.

Command Modes

SSLVPN configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The source image file for the logo is a gif, jpg, or png file that is up to 255 characters in length (filename) and up to 100 kilobytes (KB) in size. The file is referenced from a local file system, such as flash memory. An error message will be displayed if the file is not referenced from a local file system. No logo will be displayed if the image file is removed from the local file system.

Examples

The following example references mylogo.gif (from flash memory) to use as the SSL VPN logo:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# logo file flash:/mylogo.gif
Router(config-webvpn-context)#
```

In the following example, no logo is to be displayed on the login or portal pages:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# logo none
Router(config-webvpn-context)#
```

The following example configures the SSL VPN to display the default logo (Cisco) on the login and portal pages:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# logo none
Router(config-webvpn-context)#
```

Related Commands

Command	Description
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

mab

To enable MAC-based authentication on a port, use the **mab** command in interface configuration mode. To disable MAC-based authentication, use the **no** form of this command.

mab [**eap**]

no mab

Syntax Description

eap	(Optional) Configures the port to use Extensible Authentication Protocol (EAP).

Command Default

MAC-based authentication is not enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

Use the **mab** command to enable MAC-based authentication on a port. To enable EAP on the port, use the **mab eap** command.

Note If you are unsure whether MAB or MAB EAP is enabled or disabled on the switched port, use the **default mab** or **default mab eap** commands in interface configuration mode to configure MAB or MAB EAP to its default.

Examples

The following example shows how to configure MAC-based authorization on a Gigabit Ethernet port:

```
Switch(config)# interface GigabitEthernet6/2
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config-if)# mab
Switch(config-if)# end
```

Related Commands

Command	Description
show mab	Displays information about MAB.

mac access-group

To use a MAC access control list (ACL) to control the reception of incoming traffic on a Gigabit Ethernet interface, an 802.1Q VLAN subinterface, an 802.1Q-in-Q stacked VLAN subinterface, use the **mac access-group** command in interface or subinterface configuration mode. To remove a MAC ACL, use the **no** form of this command.

mac access-group *access-list-number* **in**

no mac access-group *access-list-number* **in**

Syntax Description

access-list-number	Number of a MAC ACL to apply to an interface or subinterface (as specified by a **access-list (MAC)** command). This is a decimal number from 700 to 799.
in	Filters on inbound packets.

Defaults

No access list is applied to the interface or subinterface.

Command Modes

Interface configuration (config-if)
Subinterface configuration (config-subif)

Command History

Release	Modification
12.0(32)S	This command was introduced on the Cisco 12000 series Internet router.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

MAC ACLs are applied on incoming traffic on Gigabit Ethernet interfaces and VLAN subinterfaces. After a networking device receives a packet, the Cisco IOS software checks the source MAC address of the Gigabit Ethernet, 802.1Q VLAN, or 802.1Q-in-Q packet against the access list. If the MAC access list permits the address, the software continues to process the packet. If the access list denies the address, the software discards the packet and returns an Internet Control Message Protocol (ICMP) host unreachable message.

If the specified MAC ACL does not exist on the interface or subinterface, all packets are passed.

On Catalyst 6500 series switches, this command is supported on Layer 2 ports only.

Note The **mac access-group** command is supported on a VLAN subinterface only if a VLAN is already configured on the subinterface.

Examples

The following example applies MAC ACL 101 on incoming traffic received on Gigabit Ethernet interface 0:

```
Router> enable
Router# configure terminal
```

```
Router(config)# interface gigabitethernet 0
Router(config-if)# mac access-group 101 in
```

Related Commands

Command	Description
access-list (MAC)	Defines a MAC ACL.
clear mac access-list counters	Clears the counters of a MAC ACL.
ip access-group	Configures an IP access list to be used for packets transmitted from the asynchronous host.
show access-group mode interface	Displays the ACL configuration on a Layer 2 interface.
show mac access-list	Displays the contents of one or all MAC ACLs.

mac-address (RITE)

To specify the Ethernet address of the destination host, use the **mac-address** command in router IP traffic export (RITE) configuration mode. To change the MAC address of the destination host, use the **no** form of this command.

mac-address *H.H.H*

no mac-address *H.H.H*

Syntax Description

H.H.H	48-bit MAC address.

Defaults

A destination host is not known.

Command Modes

RITE configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

The **mac-address** command, which is used to specify the destination host that is receiving the exported traffic, is part of suite of RITE configuration mode commands that are used to control various attributes for both incoming and outgoing IP traffic export.

The **ip traffic-export profile** command allows you to begin a profile that can be configured to export IP packets as they arrive or leave a selected router ingress interface. A designated egress interface exports the captured IP packets out of the router. Thus, the router can export unaltered IP packets to a directly connected device.

Examples

The following example shows how to configure the profile "corp1," which will send captured IP traffic to host "00a.8aab.90a0" at the interface "FastEthernet 0/1." This profile is also configured to export one in every 50 packets and to allow incoming traffic only from the access control lists (ACL) "ham_ACL."

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```

Related Commands

Command	Description
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.

map type

To define the mapping of an attribute in the Lightweight Directory Access Protocol (LDAP) server, use the **map type** command in attribute-map configuration mode. To remove the attribute maps, use the **no** form of this command.

map type *ldap-attr-type aaa-attr-type* [**format** *dn-to-string*]

no map type *ldap-attr-type aaa-attr-type* [**format** *dn-to-string*]

Syntax Description

ldap-attr-type	LDAP attribute type.
aaa-attr-type	Authentication, Authorization, and Accounting (AAA) attribute type.
format	(Optional) Specifies the format conversion for attribute.
dn-to-string	(Optional) Converts the distinguished name (DN) to string format.

Command Default

No mapping types are defined.

Command Modes

Attribute-map configuration (config-attr-map)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

To use the attribute mapping features, you need to understand the Cisco AAA attribute names and values as well as the LDAP servers user-defined attribute names and values.

Examples

The following example shows how to map the user-defined attribute named department to the AAA attribute named element-req-qos in an LDAP server.

```
Router(config)# ldap attribute-map att_map_1
Router(config-attribute-map)# map type department element-req-qos format dn-to-string
Router(config-attribute-map)# exit
```

Related Commands

Command	Description
attribute-map	Attaches an attribute map to a particular LDAP server.
ldap attribute-map	Configures a dynamic LDAP attribute map.
map-type	Defines the mapping of a attribute in the LDAP server.
show ldap attribute	Displays information about default LDAP attribute mapping.

mask (policy-map)

To explicitly mask specified SMTP commands or the parameters returned by the server in response to an EHLO command, use the **mask** command in global configuration mode. To remove this filter from the configuration, use the **no** form of this command:

mask

no mask

Command Default

The command-level default is not enabled.

Command Modes

Policy-map configuration mode.

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Using the **mask** command applies to certain 'match' command filters like the **match cmd** command and the **verb** keyword. Validations are performed to make this check and the configuration is not be accepted in case of invalid combinations.

Examples

The following example shows how the **mask** command is used with the **match cmd** command and **verb** keyword to prevent ESMTP inspection:

```
class-map type inspect smtp c1
    match cmd verb EHLO

policy-map type inspect smtp c1
    class type inspect smtp c1
        mask
```

Related Commands

Command	Description
match cmd	Specifies a value that limits the length of the ESMTP command line or the ESMTP command line verb used to thwart denial of service (DoS) attacks

mask-urls

To obfuscate, or mask, sensitive portions of an enterprise URL, such as IP addresses, hostnames, or port numbers, use the **mask-urls** command in webvpn group policy configuration mode. To remove the masking, use the **no** form of this command.

mask-urls

no mask-urls

Syntax Description

This command has no arguments or keywords.

Command Default

Sensitive portions of an enterprise URL are not masked.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

This command is configured in group configuration only.

Examples

The following example shows that URL obfuscation (masking) has been configured for policy group "GP":

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group GP
Router(config-webvpn-group)# mask-urls
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

match access-group

To configure the match criteria for a class map on the basis of the specified access control list (ACL), use the **match access-group** command in class-map configuration mode. To remove ACL match criteria from a class map, use the **no** form of this command.

match access-group {*access-group* | **name** *access-group-name*}

no match access-group *access-group*

Syntax Description

access-group	Numbered ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to this class. An ACL number can be a number from 1 to 2699.
name *access-group-name*	Named ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to this class. The name can be a maximum of 40 alphanumeric characters.

Command Default

No match criteria are configured.

Command Modes

Class-map configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.0(17)SL	This command was enhanced to include matching on access lists on the Cisco 10000 series router.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.4(6)T	This command was enhanced to support Zone-Based Policy Firewall.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

For class-based weighted fair queueing (CBWFQ), you define traffic classes based on match criteria including ACLs, protocols, input interfaces, quality of service (QoS) labels, and EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

Note For Zone-Based Policy Firewall, this command is not applicable to CBWFQ.

The **match access-group** command specifies a numbered or named ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

When packets are matched to an access group, a traffic rate is generated for these packets. In a zone-based firewall policy, only the first packet that creates a session matches the policy. Subsequent packets in this flow do not match the filters in the configured policy, but instead match the session directly. The statistics related to subsequent packets are shown as part of the 'inspect' action.

Supported Platforms Other than Cisco 10000 Series Routers

To use the **match access-group** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. After you identify the class, you can use one of the following commands to configure its match criteria:

- **match access-group**
- **match input-interface**
- **match mpls experimental**
- **match protocol**

Note Zone-Based Policy Firewall supports only the **match access-group**, **match protocol**, and **match class-map** commands.

If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

Note The **match access-group** command specifies the numbered access list against whose contents packets are checked to determine if they match the criteria specified in the class map. Access lists configured with the optional **log** keyword of the **access-list** command are not supported when you configure match criteria. For more information about the **access-list** command, refer to the *Cisco IOS IP Application Services Command Reference*.

Cisco 10000 Series Routers

To use the **match access-group** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish.

Note The **match access-group** command specifies the numbered access list against whose contents packets are checked to determine if they match the criteria specified in the class map. Access lists configured with the optional **log** keyword of the **access-list** command are not supported when you configure match criteria.

The following example specifies a class map called acl144 and configures the ACL numbered 144 to be used as the match criterion for that class:

```
class-map acl144
 match access-group 144
```

The following example pertains to Zone-Based Policy Firewall. The example defines a class map called c1 and configures the ACL numbered 144 to be used as the match criterion for that class.

```
class-map type inspect match-all c1
 match access-group 144
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
class-map	Creates a class map to be used for matching packets to a specified class.
match input-interface	Configures a class map to use the specified input interface as a match criterion.
match mpls experimental	Configures a class map to use the specified EXP field value as a match criterion.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.

match address (GDOI local server)

To specify an IP extended access list for a Group Domain of Interpretation (GDOI) registration, use the **match address** command in GDOI SA IPsec configuration mode. To disable the access list, use the **no** form of this command.

match address {**ipv4** *access-list-number* | *access-list-name*}

no match address {**ipv4** *access-list-number* | *access-list-name*}

Syntax Description

ipv4	Specifies that IPv4 packets should be matched.
access-list-number | *access-list-name*	Access list number or name. This value should match the access-list number or name of the extended access list that is being matched. The range is 100 through 199 or 2000 through 2699 for an expanded range.

Command Default

No access lists are matched to the GDOI entry.

Command Modes

GDOI SA IPsec configuration (gdoi-sa-ipsec)

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following example shows that the IP extended access list is 102:

```
match address ipv4 102
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration.

match address (IPSec)

To specify an extended access list for a crypto map entry, use the **match address** command in crypto map configuration mode. To remove the extended access list from a crypto map entry, use the **no** form of this command.

match address [*access-list-id* | *name*]

no match address [*access-list-id* | *name*]

Syntax Description

access-list-id	(Optional) Identifies the extended access list by its name or number. This value should match the *access-list-number* or *name* argument of the extended access list being matched.
name	(Optional) Identifies the named encryption access list. This name should match the *name* argument of the named encryption access list being matched.

Defaults

No access lists are matched to the crypto map entry.

Command Modes

Crypto map configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is required for all static crypto map entries. If you are defining a dynamic crypto map entry (with the **crypto dynamic-map** command), this command is not required but is strongly recommended.

Use this command to assign an extended access list to a crypto map entry. You also need to define this access list using the **access-list** or **ip access-list extended** commands.

The extended access list specified with this command will be used by IPSec to determine which traffic should be protected by crypto and which traffic does not need crypto protection. (Traffic that is permitted by the access list will be protected. Traffic that is denied by the access list will not be protected in the context of the corresponding crypto map entry.)

Note that the crypto access list is *not* used to determine whether to permit or deny traffic through the interface. An access list applied directly to the interface makes that determination.

The crypto access list specified by this command is used when evaluating both inbound and outbound traffic. Outbound traffic is evaluated against the crypto access lists specified by the interface's crypto map entries to determine if it should be protected by crypto and if so (if traffic matches a **permit** entry) which crypto policy applies. (If necessary, in the case of static IPSec crypto maps, new security

associations are established using the data flow identity as specified in the **permit** entry; in the case of dynamic crypto map entries, if no SA exists, the packet is dropped.) After passing the regular access lists at the interface, inbound traffic is evaluated against the crypto access lists specified by the entries of the interface's crypto map set to determine if it should be protected by crypto and, if so, which crypto policy applies. (In the case of IPSec, unprotected traffic is discarded because it should have been protected by IPSec.)

In the case of IPSec, the access list is also used to identify the flow for which the IPSec security associations are established. In the outbound case, the **permit** entry is used as the data flow identity (in general), while in the inbound case the data flow identity specified by the peer must be "permitted" by the crypto access list.

Examples

The following example shows the minimum required crypto map configuration when IKE will be used to establish the security associations. (This example is for a static crypto map.)

```
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
```

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
set peer (IPSec)	Specifies an IPSec peer in a crypto map entry.
set pfs	Specifies that IPSec should ask for perfect forward secrecy (PFS) when requesting new security associations for this crypto map entry, or that IPSec requires PFS when receiving requests for new security associations.
set security-association level per-host	Specifies that separate IPSec security associations should be requested for each source/destination host pair.
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPSec security associations.
set session-key	Specifies the IPSec session keys within a crypto map entry.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPSec)	Displays the crypto map configuration.

match authentication trustpoint

To specify the trustpoint name that should be used to authenticate the SDP peer's certificate, use the **match authentication trustpoint** command in tti-registrar configuration mode. To remove this configuration, use the **no** form of this command.

match authentication trustpoint *trustpoint-name*

no match authentication trustpoint *trustpoint-name*

Syntax Description

trustpoint-name	Specifies the truspoint name.

Command Default

No trustpoint name is specified for the iPhone deployment.

Command Modes

Tti-registrar configuration mode (tti-registrar)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **match authentication trustpoint** command can be used optionally in the SDP registrar configuration, which is used to deploy Apple iPhones on a corporate network.

If the trustpoint name is not specified, then the trustpoint configured using the **authentication trustpoint** in tti-registrar configuration mode is used to authenticate the SDP peer's certificate.

Examples

The following example configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network from global configuration mode:

```
Router(config)# crypto provisioning registrar
Router(tti-registrar)# url-profile start START
Router(tti-registrar)# url-profile intro INTRO
Router(tti-registrar)# match url /sdp/intro
Router(tti-registrar)# match authentication trustpoint apple-tp
Router(tti-registrar)# match certificate cat 10
Router(tti-registrar)# mime-type application/x-apple-aspen-config
Router(tti-registrar)# template location flash:intro.mobileconfig
Router(tti-registrar)# template variable p iphone-vpn
```

Related Commands

Command	Description
crypto provisioning registrar	Configures a device to become a registrar for the SDP exchange and enters tti-registrar configuration mode.
url-profile	Specifies a URL profile that configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network.

Command	Description
match url	Specifies the URL to be associated with the URL profile.
authentication trustpoint	Specifies the trustpoint used to authenticate the SDP petitioner device's existing certificate.
match certificate	Enters the name of the certificate map used to authorize the peer's certificate.
mime-type	Specifies the MIME type that the SDP registrar should use to respond to a request received through the URL profile.
template location	Specifies the location of the template that the SDP Registrar should use while responding to a request received through the URL profile.
template variable p	Specifies the value that goes into the OU field of the subject name in the certificate to be issued.

match body regex

To specify an arbitrary text expression to restrict specified content-types and content encoding types for text and HTML in the "body" of the e-mail, use the **match body regex** command in class-map configuration mode. To remove this match criterion, use the **no** form of this command.

match body regex *parameter-map-name*

no match body regex *parameter-map-name*

Syntax Description

parameter-map-name	Name of a specific traffic pattern specified through the **parameter-map type regex** command.

Command Default

None

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

If a match is found, possible actions that can be specified within the policy are as follows: allow, reset, or log. (The log action triggers a syslog message when a match is found.)

The text or HTML pattern is scanned only if the encoding is 7-bit or 8-bit and the encoding is checked before attempting to match the pattern. If the pattern is of another encoding type (e.g. base64, zip files etc.), then the pattern cannot be scanned

Note Using this command can impact performance because the complete SMTP connection has to be scanned.

Examples

The following example shows how to configure an SMTP policy to block an e-mail that contains the pattern "*UD-421590*" in the body of an e-mail.

```
parameter-map type regex doc-data
pattern "*UD-421590*"

class-map type inspect smtp c1
match body regex doc-data

policy-map type inspect smtp p1
class type inspect smtp c1
log
```

Related Commands

Command	Description
class-map type inspect smtp	Creates a class map for the SMTP protocol so that the match criteria is set to match criteria for this class map.
policy-map type inspect smtp	Create a Layer 7 SMTP policy map.

match certificate

To specify the name of the certificate map used to authorize the peer's certificate, use the **match certificate** command in tti-registrar configuration mode. To remove this configuration, use the **no** form of this command.

match certificate *certificate-map*

no match certificate *certificate-map*

Syntax Description

certificate-map	Specifies the certificate map name.

Command Default

No certificate map name is specified for the iPhone deployment.

Command Modes

Tti-registrar configuration mode (tti-registrar)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **match certificate** command can be used optionally in the SDP registrar configuration, which is used to deploy Apple iPhones on a corporate network.

Examples

The following example configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network from global configuration mode:

```
Router(config)# crypto provisioning registrar
Router(tti-registrar)# url-profile start START
Router(tti-registrar)# url-profile intro INTRO
Router(tti-registrar)# match url /sdp/intro
Router(tti-registrar)# match authentication trustpoint apple-tp
Router(tti-registrar)# match certificate cat 10
Router(tti-registrar)# mime-type application/x-apple-aspen-config
Router(tti-registrar)# template location flash:intro.mobileconfig
Router(tti-registrar)# template variable p iphone-vpn
```

Related Commands

Command	Description
crypto provisioning registrar	Configures a device to become a registrar for the SDP exchange and enters tti-registrar configuration mode.
url-profile	Specifies a URL profile that configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network.
match url	Specifies the URL to be associated with the URL profile.

Command	Description
match authentication trustpoint	Specifies the trustpoint name that should be used to authenticate the SDP peer's certificate in order to deploy Apple iPhones on a corporate network.
mime-type	Specifies the MIME type that the SDP registrar should use to respond to a request received through the URL profile.
template location	Specifies the location of the template that the SDP Registrar should use while responding to a request received through the URL profile.
template variable p	Specifies the value that goes into the OU field of the subject name in the certificate to be issued.

match certificate (ca-trustpoint)

To associate a certificate-based access control list (ACL) that is defined with the **crypto ca certificate map** command, use the **match certificate** command in ca-trustpoint configuration mode. To remove the association, use the **no** form of this command.

match certificate *certificate-map-label* [**allow expired-certificate | skip revocation-check | skip authorization-check**]

no match certificate *certificate-map-label* [**allow expired-certificate | skip revocation-check | skip authorization-check**]

Syntax Description

certificate-map-label	Matches the *label* argument specified in a previously defined **crypto ca certificate map** command.
allow expired-certificate	(Optional) Ignores expired certificates. **Note** If this keyword is not configured, the router does not ignore expired certificates.
skip revocation-check	(Optional) Allows a trustpoint to enforce certificate revocation lists (CRLs) except for specific certificates. **Note** If this keyword is not configured, the trustpoint enforces CRLs for all certificates.
skip authorization-check	(Optional) Skips the authentication, authorization, and accounting (AAA) check of a certificate when public key infrastructure (PKI) integration with an AAA server is configured. **Note** If this keyword is not configured and PKI integration with an AAA server is configured, the AAA checking of a certificate is done.

Defaults

If this command is not configured, no default match certificate is configured. Each of the **allow expired-certificate**, **skip revocation-check**, and **skip authorization-check** keywords have a default (see the "Syntax Description" section).

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.3(4)T	The **allow expired-certificate**, **skip revocation-check**, and **skip authorization-check** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

The **match certificate** command associates the certificate-based ACL defined with the **crypto ca certificate map** command to the trustpoint. The *certificate-map-label* argument in the **match certificate** command must match the *label* argument specified in a previously defined **crypto ca certificate map** command.

The certificate map with the label *certificate-map-label* must be defined before it can be used with the **match certificate** subcommand.

A certificate referenced in a **match certificate** command may not be deleted until all references to the certificate map are removed from configured trustpoints (that is, no **match certificate** commands can reference the certificate map being deleted).

When the certificate of a peer has been verified, the certificate-based ACL as specified by the certificate map is checked. If the certificate of the peer matches the certificate ACL, or a certificate map is not associated with the trustpoint used to verify the certificate of the peer, the certificate of the peer is considered valid.

If the certificate map does not have any attributes defined, the certificate is rejected.

Using the allow expired-certificate Keyword

The **allow expired-certificate** keyword has two purposes:

- If the certificate of a peer has expired, this keyword may be used to "allow" the expired certificate until the peer is able to obtain a new certificate.
- If your router clock has not yet been set to the correct time, the certificate of a peer will appear to be not yet valid until the clock is set. This keyword may be used to allow the certificate of the peer even though your router clock is not set.

Note

- If Network Time Protocol (NTP) is available only via the IPSec connection (usually via the hub in a hub-and-spoke configuration), the router clock can never be set. The tunnel to the hub cannot be "brought up" because the certificate of the hub is not yet valid.
- "Expired" is a generic term for a certificate that is expired or that is not yet valid. The certificate has a start and end time. An expired certificate, for purposes of the ACL, is one for which the current time of the router is outside the start and end time specified in the certificate.

Using the skip revocation-check Keyword

The type of enforcement provided using the **skip revocation-check** keyword is most useful in a hub-and-spoke configuration in which you also want to allow direct spoke-to-spoke connections. In pure hub-and-spoke configurations, all spokes connect only to the hub, so CRL checking is necessary only on the hub. If one spoke communicates directly with another spoke, the CRLs must be checked. However, if the trustpoint is configured to require CRLs, the connection to the hub to retrieve the CRL usually cannot be made because the CRL is available only via the connection hub.

Using the skip authorization-check Keyword

If the communication with an AAA server is protected with a certificate, and you want to skip the AAA check of the certificate, use the **skip authorization-check** keyword. For example, if a Virtual Private Network (VPN) tunnel is configured so that all AAA traffic goes over that tunnel, and the tunnel is protected with a certificate, you can use the **skip authorization-check** keyword to skip the certificate check so that the tunnel can be established.

The **skip authorization-check** keyword should be configured after PKI integration with an AAA server is configured.

Examples

The following example shows a certificate-based ACL with the label "Group" defined in a **crypto ca certificate map** command and included in the **match certificate** command:

```
crypto ca certificate map Group 10
 subject-name co ou=WAN
 subject-name co o=Cisco
!
crypto ca trustpoint pki
 match certificate Group
```

The following example shows a configuration for a central site using the **allow expired-certificate** keyword. The router at a branch site has an expired certificate named "branch1" and has to establish a tunnel to the central site to renew its certificate.

```
crypto pki trustpoint VPN-GW
 enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
 serial-number none
 fqdn none
 ip-address none
 subject-name o=Home Office Inc,cn=Central VPN Gateway
 revocation-check crl
 match certificate branch1 allow expired-certificate
```

The following example shows a branch office configuration using the **skip revocation-check** keyword. The trustpoint is being allowed to enforce CRLs except for "central-site" certificates.

```
crypto pki trustpoint home-office
 enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
 serial-number none
 fqdn none
 ip-address none
 subject-name o=Home Office Inc,cn=Branch 1
 revocation-check crl
 match certificate central-site skip revocation-check
```

The following example shows a branch office configuration using the **skip authorization-check** keyword. The trustpoint is being allowed to skip AAA checking for the central site.

```
crypto pki trustpoint home-office
 auth list allow_list
 auth user subj commonname
 match certificate central-site skip authorization-check
```

Related Commands

Command	Description
crypto ca certificate map	Defines certificate-based ACLs.
crypto ca trustpoint	Declares the CA that your router should use.

match certificate (ISAKMP)

To assign an Internet Security Association Key Management Protocol (ISAKMP) profile to a peer on the basis of the contents of arbitrary fields in the certificate, use the **match certificate** command in crypto ISAKMP profile configuration mode. To remove the profile, use the **no** form of this command.

match certificate *certificate-map*

no match certificate *certificate-map*

Syntax Description

certificate-map	Name of the certificate map.

Defaults

No default behavior or values

Command Modes

Crypto ISAKMP profile configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SX	This command is supported in the Cisco 12.2SX family of releases. Support in a 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

The **match certificate** command is used after the certificate map has been configured and the ISAKMP profiles have been assigned to them.

Examples

The following configuration example shows that whenever a certificate contains “ou = green,” the ISAKMP profile “cert_pro” will be assigned to the peer.

```
crypto pki certificate map cert_map 10
 subject-name co ou = green
!
!
crypto isakmp identity dn
crypto isakmp profile cert_pro
   ca trust-point 2315
   ca trust-point LaBcA
   initiate mode aggressive
   match certificate cert_map
```

Related Commands

Command	Description
client configuration group	Associates a group with the peer that has been assigned an ISAKMP profile.

match certificate override cdp

To manually override the existing certificate distribution point (CDP) entries for a certificate with a URL or directory specification, use the **match certificate override cdp** command in ca-trustpoint configuration mode. To remove the override, use the **no** form of this command.

match certificate *certificate-map-label* **override cdp** {**url** | **directory**} *string*

no match certificate *certificate-map-label* **override cdp** {**url** | **directory**} *string*

Syntax Description

certificate-map-label	A user-specified label that must match the *label* argument specified in a previously defined **crypto ca certificate map** command.
url	Specifies that the certificates CDPs will be overridden with an http or ldap URL.
directory	Specifies that the certificate's CDPs will be overridden with an ldap directory specification.
string	The URL or directory specification.

Defaults

The existing CDP entries for the certificate are used.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

Use the **match certificate override cdp** command to replace all of the existing CDPs in a certificate with a manually configured CDP URL or directory specification.

The *certificate-map-label* argument in the **match certificate override cdp** command must match the *label* argument specified in a previously defined **crypto ca certificate map** command.

Note Some applications may time out before all CDPs have been tried and will report an error message. This will not affect the router, and the Cisco IOS software will continue attempting to retrieve a CRL until all CDPs have been tried.

Examples

The following example uses the **match certificate override cdp** command to override the CDPs for the certificate map named Group1 defined in a **crypto ca certificate map** command:

```
crypto ca certificate map Group1 10
 subject-name co ou=WAN
 subject-name co o=Cisco
!
crypto ca trustpoint pki
 match certificate Group1 override cdp url http://server.cisco.com
```

Related Commands

Command	Description
crypto ca certificate map	Defines certificate-based ACLs.
crypto ca trustpoint	Declares the CA that your router should use.

match certificate override ocsp

To override an Online Certificate Status Protocol (OCSP) server setting specified in either the Authority Info Access (AIA) field of the client certificate or in the trustpoint configuration, use the **match certificate override ocsp** command in ca-trustpoint configuration mode. To remove the OCSP server override setting, use the **no** form of this command.

match certificate *certificate-map-label* **override ocsp** [**trustpoint** *trustpoint-label*] *sequence-number* **url** *ocsp-url*

no match certificate *certificate-map-label* **override ocsp** [**trustpoint** *trustpoint-label*] *sequence-number* **url** *ocsp-url*

Syntax Description

certificate-map-label	Specifies the exact name of an existing certificate map label.
trustpoint *trustpoint-label*	(Optional) Specifies the existing trustpoint to be used when validating the OCSP server responder certificate.
sequence-number	Indicates the order of the override statements to be applied when a certificate is being verified. **Note** Certificate matches are performed from the lowest sequence number to the highest sequence number. If more than one command is issued with the same sequence number, the previous OCSP server override setting is replaced.
url *ocsp-url*	Specifies the OCSP server URL.

Command Default

No override OSCP server setting will be configured.

Command Modes

Ca-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

OCSP server validation is usually based on the root certification authority (CA) certificate or a valid subordinate CA certificate, but may also be configured for validation of the OCSP server identity with the **match certificate override ocsp** command and **trustpoint** keyword.

One or more OCSP servers may be specified, either per client certificate or per group of client certificates. When the certificate matches a configured certificate map, the AIA field of the client certificate and any previously issued **ocsp url** command settings are overwritten with the specified OCSP server. If the **ocsp url** configuration exists and no map-based match occurs, the **ocsp url** configuration settings will continue to apply to the client certificates.

Examples

The following example shows an excerpt of the running configuration output when adding an override OCSP server to the beginning of an existing sequence:

```
match certificate map3 override ocsp 5 url http://192.168.2.3/
show running-config
.
.
.
        match certificate map3 override ocsp 5 url http://192.168.2.3/
        match certificate map1 override ocsp 10 url http://192.168.2.1/
        match certificate map2 override ocsp 15 url http://192.168.2.2/
```

The following example shows an excerpt of the running configuration output when an existing override OSCP server is replaced and a trustpoint is specified to use an alternative public key infrastructure (PKI) hierarchy:

```
match certificate map4 override ocsp trustpoint tp4 10 url http://192.168.2.4/newvalue\
show running-config
.
.
.
        match certificate map3 override ocsp trustpoint tp3 5 url http://192.168.2.3/
        match certificate map1 override ocsp trustpoint tp1 10 url http://192.168.2.1/
        match certificate map4 override ocsp trustpoint tp4 10 url
http://192.168.2.4/newvalue
        match certificate map2 override ocsp trustpoint tp2 15 url http://192.168.2.2/
```

The following example shows an excerpt of the running configuration output when an existing override OCSP server is removed from an existing sequence:

```
no match certificate map1 override ocsp trustpoint tp1 10 url http://192.168.2.1/
show running-config
.
.
.
        match certificate map3 override ocsp trustpoint tp3 5 url http://192.168.2.3/
        match certificate map4 override ocsp trustpoint tp4 10 url
http://192.168.2.4/newvalue
        match certificate map2 override ocsp trustpoint tp2 15 url http://192.168.2.2/
```

Related Commands

Command	Description
crypto pki certificate map	Defines values in a certificate that should be matched or not matched.
ocsp url	Specifies the URL of an OCSP server so that the trustpoint can check the certificate status.

match certificate override sia

To manually override the existing SubjectInfoAccess (SIA) attribute, use the **match certificate override sia** command in CA-trustpoint configuration mode. To remove the override, use the **no** form of this command.

match certificate *certificate-map-label* **override sia** *sequence-number certificate-url*

no match certificate *certificate-map-label* **override sia**

Syntax Description

certificate-map-label	A user-specified label that should match the label argument specified in a previously defined **crypto ca certificate map** command.
sequence-number	The order of the override statements to be applied when a certificate is being verified. **Note** Certificate matches are performed from the lowest sequence number to the highest sequence number. If more than one command is issued with the same sequence number, the previous SIA override setting is replaced.
certificate-url	The remote location of the certificate in URL format.

Command Default

The existing SIA entries for the certificate are used.

Command Modes

CA-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The certificate's storage location is contained in the certificate itself by the issuing authority. This data is contained in the SIA and the AuthorityInfoAccess (AIA) extension in certificates. Use the **match certificate override sia** command to manually configure the remote location of the identity certificate regardless of the SIA attribute in the certificate.

Examples

The following example shows how to use the **match certificate override sia** command to override the SIAs for the certificate map named Group1 defined in a **crypto ca certificate map** command:

```
Router(config)# crypto ca certificate map Group1 10
Router(ca-certificate-map)# subject-name co ou=WAN
Router(ca-certificate-map)# subject-name co o=Cisco
!
Router(config)# crypto ca trustpoint pki
Router (ca-trustpoint)# match certificate Group1 override sia 100
http://certs.example.com/certificate.cer
```

Related Commands

Command	Description
crypto ca certificate map	Defines certificate-based ACLs.
crypto ca trustpoint	Declares the CA that your router should use.

match class-map

To use a traffic class as a classification policy, use the **match class-map** command in class-map configuration mode. To remove a specific traffic class as a match criterion, use the **no** form of this command.

match class-map *class-map-name*

no match class-map *class-map-name*

Syntax Description

class-map-name	Name of the traffic class to use as a match criterion.

Command Default

No match criteria are specified.

Command Modes

Class-map configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.4(6)T	This command was enhanced to support Zone-Based Policy Firewall.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was implemented on the Cisco 10000 series.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

The only method of including both match-any and match-all characteristics in a single traffic class is to use the **match class-map** command. To combine match-any and match-all characteristics into a single class, do one of the following:

- Create a traffic class with the match-any instruction and use a class configured with the match-all instruction as a match criterion (using the **match class-map** command).
- Create a traffic class with the match-all instruction and use a class configured with the match-any instruction as a match criterion (using the **match class-map** command).

You can also use the **match class-map** command to nest traffic classes within one another, saving users the overhead of re-creating a new traffic class when most of the information exists in a previously configured traffic class.

When packets are matched to a class map, a traffic rate is generated for these packets. In a zone-based firewall policy, only the first packet that creates a session matches the policy. Subsequent packets in this flow do not match the filters in the configured policy, but instead match the session directly. The statistics related to subsequent packets are shown as part of the 'inspect' action.

Examples

Non-Zone-Based Policy Firewall Examples

In the following example, the traffic class called class1 has the same characteristics as traffic class called class2, with the exception that traffic class class1 has added a destination address as a match criterion. Rather than configuring traffic class class1 line by line, you can enter the **match class-map class2** command. This command allows all of the characteristics in the traffic class called class2 to be included in the traffic class called class1, and you can simply add the new destination address match criterion without reconfiguring the entire traffic class.

```
Router(config)# class-map match-any class2
Router(config-cmap)# match protocol ip
Router(config-cmap)# match qos-group 3
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit

Router(config)# class-map match-all class1
Router(config-cmap)# match class-map class2
Router(config-cmap)# match destination-address mac 1.1.1
Router(config-cmap)# exit
```

The following example shows how to combine the characteristics of two traffic classes, one with match-any and one with match-all characteristics, into one traffic class with the **match class-map** command. The result of traffic class called class4 requires a packet to match one of the following three match criteria to be considered a member of traffic class called class 4: IP protocol *and* QoS group 4, destination MAC address 1.1.1, or access group 2. Match criteria IP protocol *and* QoS group 4 are required in the definition of the traffic class named class3 and included as a possible match in the definition of the traffic class named class4 with the **match class-map class3** command.

In this example, only the traffic class called class4 is used with the service policy called policy1.

```
Router(config)# class-map match-all class3
Router(config-cmap)# match protocol ip
Router(config-cmap)# match qos-group 4
Router(config-cmap)# exit

Router(config)# class-map match-any class4
Router(config-cmap)# match class-map class3
Router(config-cmap)# match destination-address mac 1.1.1
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit

Router(config)# policy-map policy1
Router(config-pmap)# class class4
Router(config-pmap-c)# police 8100 1500 2504 conform-action transmit exceed-action
set-qos-transmit 4
Router(config-pmap-c)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.

match class session

To configure match criteria for a class map used to identify a session (flow) containing packets of interest, which is then applied to all packets transmitted during the session, use the **match class session** command in class map configuration mode. To remove this configuration, use the **no** form of this command.

match class *class-name* [**packet-range** *low high* | **byte-range** *low high*] **session**

no match class *class-name* [**packet-range** *low high* | **byte-range** *low high*] **session**

Syntax Description

class-name	Specifies the class map used to identify a session containing packets of interest. The classification results are preserved for the subsequent packets of the same packet session.
packet-range *low high*	(Optional) Specifies the range of packets from 1 to 2147483647, in which the regular expressions (regex) within every packet is are checked. The classification results are preserved for the specified packets or bytes of the same packet session.
byte-range *low high*	(Optional) Specifies the range of bytes from 1 to 2147483647, in which the regular expressions (regex) within every packet are checked. The classification results are preserved for the specified packets or bytes of the same packet session.

Command Default

The regex matching is within a single packet with a range 1 to infinity.

Command Modes

Class map configuration (config-cmap)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

With the introduction of Cisco IOS Release15.1(3)T, Flexible Packet Matching (FPM) can now match every packet against the filters specified in the class map and pass the match result to consecutive packets of the same network session. If a filter matches with malicious content in the packet's protocol header or payload, then the required action is taken to resolve the problem.

The **match class session** command configures match criteria that identify a session containing packets of interest, which is then applied to all packets transmitted during the session. The **packet-range** and **byte-range** keywords are used to create a filter mechanism that increases the performance and matching accuracy of regex-based FPM class maps by classifying traffic that resides in the narrow packet number or byte ranges of each packet flow. If packets go beyond the classification window, then the packet flow can be identified as unknown and packet classification is terminated early to increase performance. For example, a specific application can be blocked efficiently by filtering all packets that belong to this application on a session. These packets are dropped without matching every individual packet with the filters, which improves the performance of a session.

These filters also reduce the number of false positives introduced by general regex-based approaches. For example, Internet company messenger traffic can be classified with a string like **intco**, **intcomsg**, and **ic**. These strings are searched for in a packet's payload. These small strings can appear in the packet payload of any other applications, such as e-mail, and can introduce false positives. False positives can be avoided by specifying which regex is searched within which packet of a particular packet flow.

Once the match criteria are applied to packets belonging to the specific traffic class, these packets can be discarded by configuring the **drop all** command in a policy map. Packets match only on the packet flow entry of an FPM, and skip user-configured classification filters.

A match class does not have to be applied exclusively for a regex-based filter. Any FPM filter can be used in the nested match class filter. For example, if the match class **c1** has the filter **match field TCP source-port eq 80**, then the **match class c1 session** command takes the same action for the packets that follow the first matching packet.

Examples

The following example shows how to configure a class map and policy map to specify the protocol stack class, the match criteria and action to take, and a combination of classes using session-based (flow-based) and nonsession-based actions. The **drop all** command is associated with the action to be taken on the policy.

```
Router(config)# class-map type access-control match-all my-HTTP
Router(config-cm)# match field tcp destport eq 8080
Router(config-cm)# match start tcp payload-start offset 20 size 10 regex "GET"

Router(config)# class-map type access-control match-all my-FTP
Router(config-cmap)# match field tcp destport eq 21

Router(config)# class-map type access-control match all class1
Router(config-cmap)# match class my-HTTP session
Router(config-cmap)# match start tcp payload-start offset 40 size 20 regex "abc.*def"

Router(config)# policy-map type access-control my_http_policy
Router(config-pmap)# class class1
Router(config-pmap-c)# drop all

Router(config)# interface gigabitEthernet 0/1
Router(config-if)# service-policy type access-control input my_http_policy
```

The following example shows how to configure a class map and policy map to specify the protocol stack class, the match criteria and action to take, and a combination of classes using session-based (flow-based) and nonsession-based actions. However, this example uses the **match class** command with the **packet-range** keyword, which acts as a filter mechanism to increases the performance and matching accuracy of the regex-based FPM class map.

```
Router(config)# load disk2:ip.phdf
Router(config)# load protocol disk2:tcp.phdf

Router(config)# class-map type stack match-all ip_tcp
Router(config-cmap)# description "match TCP over IP packets"
Router(config-cmap)# match field ip protocol eq 6 next tcp

Router(config)# class-map type access-control match-all WM
Router(config-cmap) # match start tcp payload-start offset 20 size 20 regex
".*(WEBCO|WMSG|WPNS).......[LWT].*\xc0\x80"

Router(config)# class-map type access-control match-all wtube
Router(config-cmap) # match start tcp payload-start offset 20 size 20 regex
".*GET\x20.*HTTP\x2f(0\.9|1\.0|1\.1)\x0d\x0aHost:\x20webtube.com\x0d\x0a"
```

```
Router(config)# class-map type access-control match-all doom
Router(config-cmap) # match start tcp payload-start offset 20 size 20 string virus

Router(config)# class-map type access-control match-all class_webco
Router(config-cmap)# match class WM session
Router(config-cmap)# match field ip length eq 0x194
Router(config-cmap)# match start network-start offset 224 size 4 eq 0x4011010

Router(config)# class-map type access-control match-all class_webtube
Router(config-cmap)# match class wtube packet-range 1 5 session
Router(config-cmap)# match class doom session
Router(config-cmap)# match field ip length eq 0x194
Router(config-cmap)# match start network-start offset 224 size 4 eq 0x4011010

Router(config)# policy-map type access-control my_policy
Router(config-pmap)# class class_webco
Router(config-pmap-c)# log

Router(config)# policy-map type access-control my_policy
Router(config-pmap)# class class_webtube
Router(config-pmap-c)# drop all

Router(config)# policy-map type access-control P1
Router(config-pmap)# class ip_tcp
Router(config-pmap-c)# service-policy my_policy

Router(config)# interface gigabitEthernet 0/1
Router(config-if)# service-policy type access-control input P1
```

Related Commands

Command	Description
drop	Configures a traffic class to discard packets belonging to a specific class.
log	Generates log messages for the traffic class.

match cmd

To specify a value that limits the length of the ESMTP command line or specifies the ESMTP command line verb used to thwart denial of service (DoS) attacks, use the **match cmd** command in class-map configuration mode. To disable this inspection parameter, use the **no** form of this command.

match cmd {**line length gt** *length* | **verb** {**AUTH** | **DATA** | **EHLO** | **ETRN** | **EXPN** | **HELO** | **HELP** | **MAIL NOOP** | **QUIT** | **RCPT** | **RSET** | **SAML** | **SEND** | **SOML** | **STARTTLS** | **VERB** | **VRFY** | **WORD**}}

no match cmd {**line length gt** *length* | **verb** {**AUTH** | **DATA** | **EHLO** | **ETRN** | **EXPN** | **HELO** | **HELP** | **MAIL NOOP** | **QUIT** | **RCPT** | **RSET** | **SAML** | **SEND** | **SOML** | **STARTTLS** | **VERB** | **VRFY** | **WORD**}}

Syntax Description

line length gt *length*	Specifies the ESMTP command line greater than the length of a number of characters from 1 to 65535.
verb	Specifies the ESMTP command verb used to thwart DoS attacks.
AUTH	SMTP service extension whereby an SMTP client may indicate an authentication mechanism to the server, perform an authentication protocol exchange, and optionally negotiate a security layer for subsequent protocol interactions.
DATA	Sent by a client to initiate the transfer of message content.
EHLO	Enables the server to identify its support for Extended Simple Mail Transfer Protocol (ESMTP) commands.
ETRN	Requests the local SMTP server to initiate delivery of mail to the external SMTP server on a separate SMTP connection.
EXPN	Expand a mailing list address into individual recipients. Often disabled to prevent use by spammers.
HELO	Sent by a client to identify itself, usually with a domain name.
HELP	Returns a list of commands that are supported by the SMTP service.
MAIL NOOP	Start of MAIL FROM: Identifies sender of mail message. May be forged. May not correspond to the From: line in a mail message. Should be added in Return Path header. Address to send any undeliverable notifications (bounces). The NO OPeration (NOOP) does nothing, except keep the connection active and help synchronize commands and responses.
QUIT	Terminates the session.
RCPT	Identifies the message recipients; used in the form RCPT TO:
RSET	Nullifies the entire message transaction and resets the buffer.
SAML	Start of SAML FROM: Like MAIL except supposed to also display the message on the recipients computer (early form of instant messaging).
SOML	Start of SAML FROM: Like MAIL except supposed to either mail the message OR display the message on the recipients computer (early form of instant messaging)
STARTTLS	Triggers start of TLS negotiation for secure SMTP conversation. If successful, resets state to before EHLO command sent.
VERB	Enables verbose (detailed) responses.

VRFY	Verifies that a mailbox is available for message delivery; for example, the **VRFY MARK** command verifies that a mailbox for MARK resides on the local server. This command is off by default in Exchange implementations.
WORD	Specifies a word in the body of the e-mail message.

Command Default

The length of the ESMTP command line or command line verb is not defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

In a **class-map type inspect smtp match-all** command statement with the **match cmd verb** command statement, only the following **match cmd line length gt** command statement can coexist. For example:

```
class-map type inspect smtp match-all c2
  match cmd line length gt 256
  match cmd verb MAIL
```

Note There are no match restrictions in case of a **class-map type inspect smtp match-any** command statement for a class map because the class-map applies to all SMTP commands.

The class-map **c2** matches if the length of only the e-mail command is greater than 256 bytes (which is not applicable to other commands), which translates to: If the length of the MAIL command exceeds the configured value.

Note If no **match cmd verb** command statement is specified in a **class-map type inspect smtp match-all** command statement for a class-map, which contains the **match cmd line length gt** command statement, then the class-map applies to all SMTP commands.

Examples

The following example shows how to configure an SMTP application firewall policy to limit the length of an SMTP command line to prevent a Denial of Service (DoS) attack:

```
class-map type inspect smtp c1
 match header length gt 16000
```

Related Commands

Command	Description
class-map type inspect smtp	Creates a class map for the SMTP protocol so that the match criteria is set to match criteria for this class map.

match data-length

To determine if the amount of data transferred in a Simple Mail Transfer Protocol (SMTP) connection is greater than the configured limit, use the **match data-length** command in class-map type inspect smtp configuration mode. To remove this match criteria, use the **no** form of this command.

match data-length gt *max-data-value*

no match data-length gt *max-data-value*

Syntax Description

gt *max-data-value*	Maximum number of bytes (data) that can be transferred in a single SMTP session. After the maximum value is exceeded, the firewall logs an alert message and closes the session. The default is 20.

Command Default

The inspection rule is not defined.

Command Modes

Class-map type inspect smtp configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

The **match data-length** match criteria can be specified only under an SMTP class map. For more information, see the **class-map type inspect smtp** command.

Examples

The following example specifies that a maximum of 200000 bytes can be transferred in a single SMTP session:

```
class-map type inspect smtp c11
 match data-length gt 200000

policy-map type inspect smtp p11
 class type inspect smtp c11
  reset
```

Related Commands

Command	Description
class-map type inspect smtp	Configures inspection parameters for SMTP.
ip inspect name	Defines a set of inspection rules.

match encrypted

To configure the match criteria for a class map on the basis of encrypted Flexible Packet Matching (FPM) filters and enter FPM match encryption filter configuration mode, use the **match encrypted** command in class-map configuration mode. To remove the specified match criteria, use the **no** form of this command.

match encrypted

no match encrypted

Syntax Description

This command has no arguments or keywords.

Command Default

No match criteria are configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

If you have access to an encrypted traffic classification definition file (eTCDF) or if you know valid values to configure encrypted Flexible Packet Matching (FPM) filters, you can configure the same eTCDF through the command-line interface instead of using the preferred method of loading the eTCDF on the router. You must create a class map of type access-control using the **class-map type** command, and use the **match encrypted** command to configure the match criteria for the class map on the basis of encrypted FPM filters and enter FPM match encryption filter configuration mode. You can then use the appropriate commands to specify the algorithm, cipher key, cipher value, filter hash, filter ID, and filter version. You can copy the values from the eTCDF by opening the eTCDF in any text editor.

Examples

The following example shows how to enter FPM match encryption filter configuration mode:

```
Router(config)# class-map type access-control match-all class2
Routre(config-cmap)# match encrypted
Router(c-map-match-enc-config)#
```

Related Commands

Command	Description
algorithm	Specifies the algorithm to be used for decrypting the filters.
cipherkey	Specifies the symmetric keyname that is used to decrypt the filter.
ciphervalue	Specifies the encrypted filter contents.
class-map type	Creates a class map to be used for matching packets to a specified class.
filter-hash	Specifies the hash for verification and validation of decrypted contents.

Command	Description
filter-id	Specifies a filter level ID for encrypted filters.
filter-version	Specifies the filter level version value for encrypted filters.

match file-transfer

To use file transfers as the match criterion, use the **match file-transfer** command in class-map configuration mode. To remove the file transfer match criterion from the configuration file, use the **no** form of this command.

match file-transfer [*regular-expression*]

no match file-transfer [*regular-expression*]

Syntax Description

regular-expression	(Optional) The regular expression used to identify file transfers for a specified P2P application. For example, entering ".exe" as the regular expression would classify the Gnutella file transfer connections containing the string ".exe" as matches for the traffic policy. To specify that all file transfer connections be identified by the traffic class, use an asterisk (*) as the regular expression.

Command Default

None

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

After the **class-map type inspect** command is issued and a P2P application is specified, you can use the **match file-transfer** command to configure the Cisco IOS Firewall to match file transfer connections within any supported P2P protocol.

Note This command can be used only with the following supported P2P protocols: eDonkey, Gnutella, Kazaa Version 2, and FastTrack.

Examples

The following example shows how to configure the Cisco IOS Firewall to block and reset all Gnutella file transfers that are classified into the "my-gnutella-restrictions" class map:

```
class-map type inspect gnutella match-any my-gnutella-restrictions
 match file-transfer *
!
policy-map type inspect p2p my-p2p-policy
 reset
 log
```

Related Commands

Command	Description
class-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect type class map.

match header count

To configure an HTTP firewall policy to permit or deny HTTP traffic on the basis of request, response, or both request and response messages whose headers do not exceed a maximum number of fields, use the **match header count** command in class-map configuration mode. To change the configuration, use the **no** form of this command.

match {**request** | **response** | **req-resp**} **header** [*header-name*] **count gt** *number*

no match {**request** | **response** | **req-resp**} **header** [*header-name*] **count gt** *number*

Syntax Description

request	Headers in request messages are checked for the match criterion.
response	Headers in response messages are checked for the match criterion.
req-resp	Headers in both request and response messages are checked for the match criterion.
header-name	(Optional) Specific line in the header field. This argument enables the firewall to scan for repeated header fields. **Note** If this option is defined, the **gt** *number* option must be set to 1.
gt *number*	Message cannot be greater than the specified number of header lines (fields).

Command Default

HTTP header-lines are not considered when permitting or denying HTTP traffic.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Use the **match header count** command to configure an HTTP firewall policy match criterion on the basis of a maximum allowed header fields count.

If a match is found, possible actions that can be specified within the policy are as follows: allow, reset, or log. (The log action triggers a syslog message when a match is found.)

Header Field Repetition Inspection

To enable the firewall policy to checks whether a request or response message has repeated header fields, use the *header-name* argument. This functionality can be used to prevent session smuggling.

Examples

The following example shows how to configure an HTTP application firewall policy to block all requests that exceed 16 header fields:

```
class-map type inspect http hdr_cnt_cm
 match req-resp header count gt 16

policy-map type inspect http hdr_cnt_pm
 class type inspect http hdr_cnt_cm
 reset
```

The following example shows how to configure an HTTP application firewall policy to block a request or response that has multiple content-length header lines:

```
class-map type inspect http multi_occrns_cm
 match req-resp header content-length count gt 1

policy-map type inspect http multi_occrns_pm
 class type inspect http multi_occrns_cm
 reset
```

match header length gt

To thwart DoS attacks, use the **match header length gt** command in class-map configuration mode. To disable this inspection parameter, use the **no** form of this command.

match header length gt *bytes*

no match length gt *bytes*

Syntax Description

bytes	Specifies a value from 1 to 65535 that limits the maximum length of the SMTP header in bytes.

Command Default

Header length is not considered when permitting or denying SMTP messages.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(9)T	The *header-name* argument and the **req-resp** keyword were added.
12.4(20)T	The **request**, **response**, and **req-resp** keywords were removed and the *header-name* argument was removed. This command now applies to SMTP only.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

The **match header length** command matches on the maximum length of an SMTP header. If that number is exceeded, the match succeeds.

If a match is found, possible actions that can be specified within the policy are as follows: allow, reset, or log. (The log action triggers a syslog message when a match is found.)

Examples

The following example shows how to configure an SMTP application firewall policy to block all SMTP headers that exceed a length of 4096 bytes:

```
class-map type inspect smtp c1
 match header length gt 4096

policy-map type inspect smtp p1
 class type inspect smtp c1
 reset
```

Related Commands

Command	Description
max-header-regex	Specifies an arbitrary text expression in the SMTP e-mail message header (subject field) or e-mail body such as ‘subject’, ‘Received’, ‘To’ or other private header fields to monitor text patterns.

match header regex

To specify an arbitrary text expression (regular expression) in message or content type headers to monitor text patterns, use the **match header regex** command in class map configuration mode. To remove this filter from the configuration, use the **no** form of this command.

Note The **request**, **response**, and **req-resp** keywords and *header-name* argument are not used in the configuration of an SMTP class map.

match {**request | response | req-resp**} **header** [*header-name*] **regex** *parameter-map-name*

no match {**request | response | req-resp**} **header** [*header-name*] **regex** *parameter-map-name*

Syntax Description

request	Headers in request messages are checked for the match criterion.
response	Headers in response messages are checked for the match criterion.
req-resp	Headers in both request and response messages are checked for the match criterion.
header-name	Specific line or content type in the header field. This argument enables the firewall to scan for repeated header fields.
parameter-map-name	Name of a specific traffic pattern specified through the **parameter-map type regex** command.

Command Default

Policies do not monitor content type headers.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.4(20)T	The **request**, **response**, and **req-resp** keywords and *header-name* argument were removed for the configuration of an SMTP class map.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

Configuring a Class Map for SMTP

Use the **match header regex** command to configure an SMTP policy match criterion on the basis of headers that match the regular expression defined in a parameter map. An arbitrary text expression in the SMTP e-mail message header (subject field) or e-mail body such as ‘subject’, ‘Received’, ‘To’ or other private header fields helps the router to monitor text patterns.

Configuring a Class Map for HTTP

An HTTP firewall policy match criteria can be configured on the basis of headers that match the regular expression defined in a parameter map.

HTTP has two regular expression (regex) options. One combines the **header** keyword, content type header name, and **regex** keyword and *parameter-map-name* argument. The other combines the **header** keyword and **regex** keyword and *parameter-map-name* argument.

- If the **header** and **regex** keywords are used with the *parameter-map-name* argument, it does not require a period and asterisk infront of the *parameter-map-name* argument. For example, either "html" or ".*html" *parameter-map-name* argument can be configured.
- If the **header** keyword is used with the **content-type** header name and **regex** keyword, then the parameter map name requires a period and asterisk (.*) in front of the *parameter-map-name* argument. For example, the *parameter-map-name* argument “html” is expressed as: .*html

Note If the period and asterisk is added in front of html (.*html), the *parameter-map-name* argument works for both HTTP regex options.

- The **mismatch** keyword is only valid for the **match response header content-type regex** command syntax for messages that need to be matched that have a **content-type** header name mismatch.

Tip It is a good practice to add ".*" to the **regex** *parameter-map-name* arguments that are not present at the beginning of a text string.

Examples

SMTP Class Map Example

The following example shows how to configure an SMTP policy using the **match header regex** command:

```
parameter-map type regex lottery-spam
 pattern "Subject:*lottery*"

class-map type inspect smtp c1
 match header regex lottery-spam

policy-map type inspect smtp p1
 class type inspect smtp c1
 reset
```

HTTP Class Map Example

The following example shows how to configure an HTTP policy using the **match header regex** command:

```
parameter-map type inspect .*html

class-map type inspect http http-class
 match req-resp header regex .*html

policy-map type inspect http myhttp-policy
 class-type inspect http http-class
 reset
```

Related Commands

Command	Description
max-header-regex	Specifies an arbitrary text expression in the SMTP e-mail message header (subject field) or e-mail body such as ‘subject’, ‘Received’, ‘To’ or other private header fields to monitor text patterns.
parameter-map type	Creates or modifies a parameter map.
policy-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (protocol-specific) inspect type policy map.

match identity

To match an identity from a peer in an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **match identity** command in ISAKMP profile configuration mode. To remove the identity, use the **no** form of this command.

match identity {**group** *group-name* | **address** {*address* [*mask*] [*fvrf*] | **ipv6** *ipv6-address*} | **host** *host-name* | **host domain** *domain-name* | **user** *user-fqdn* | **user domain** *domain-name*}

no match identity {**group** *group-name* | **address** {*address* [*mask*] [*fvrf*] | **ipv6** *ipv6-address*} | **host** *host-name* | **host domain** *domain-name* | **user** *user-fqdn* | **user domain** *domain-name*}

Syntax Description

group *group-name*	A Unity group that matches identification (ID) type ID_KEY_ID. If Unity and main mode Rivest, Shamir, and Adelman (RSA) signatures are used, the *group-name* argument matches the Organizational Unit (OU) field of the Distinguished Name (DN).
address *address* [*mask*] [*fvrf*]	Identity that matches the identity of type ID_IPV4_ADDR. • *mask*—Use to match the range of the address. • *fvrf*—Use to match the address in the front door Virtual Route Forwarding (FVRF) Virtual Private Network (VPN) space.
ipv6 *ipv6-address*	Identity that matches the identity of type ID_IPV6_ADDR.
host *host-name*	Identity that matches an identity of the type ID_FQDN.
host domain *domain-name*	Identity that matches an identity of the type ID_FQDN, whose fully qualified domain name (FQDN) ends with the domain name.
user *user-fqdn*	Identity that matches the FQDN.
user domain *domain-name*	Identity that matches the identities of the type ID_USER_FQDN. When the **user domain** keyword is present, all users having identities of the type ID_USER_FQDN and ending with "*domain-name*" will be matched.

Command Default

No default behavior or values

Command Modes

ISAKMP profile configuration (conf-isa-prof)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(4)T	The **ipv6** keyword and *ipv6-address a*rgument were added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

There must be at least one **match identity** command in an ISAKMP profile configuration. The peers are mapped to an ISAKMP profile when their identities are matched (as given in the ID payload of the Internet Key Exchange [IKE] exchange) against the identities that are defined in the ISAKMP profile. To uniquely map to an ISAKMP profile, no two ISAKMP profiles should match the same identity. If the peer identity is matched in two ISAKMP profiles, the configuration is invalid.

Examples

The following example shows that the **match identity** command is configured:

```
crypto isakmp profile vpnprofile
 match identity group vpngroup
 match identity address 10.53.11.1
 match identity host domain example.com
 match identity host server.example.com
```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile and audits IPSec user sessions.

match (IKEv2 policy)

To match a policy based on Front-door VPN Routing and Forwarding (FVRF) or local parameters, such as an IP address, use the **match** command in IKEv2 policy configuration mode. To delete a match, use the **no** form of this command.

match address local {*ipv4-address* | *ipv6-address* | **fvrf** *fvrf-name* | **any**}

no match address local {*ipv4-address* | *ipv6-address* | **fvrf** *fvrf-name* | **any**}

Syntax Description

address local	Matches a policy based on the local IPv4 or IPv6 address.
ipv4-address	IPv4 address.
ipv6-address	IPv6 address.
fvrf	Matches a policy based on the user-defined FVRF.
frvf-name	FVRF name
any	Matches a policy based on any FVRF.

Command Default

If no match address is specified, the policy matches all local addresses.

Command Modes

IKEv2 policy configuration (crypto-ikev2-policy)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. Support was added for IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to match a policy based on the FVRF or the local IP address (IPv4 or IPv6). The FVRF specifies the VRF in which the IKEv2 security association (SA) packets are negotiated. The default FVRF is the global FVRF. Use the **match fvrf any** command to match a policy based on any FVRF.

A policy with no match address local statement will match all local addresses. A policy with no match FVRF statement will match the global FVRF. If there are no match statements, an IKEv2 policy matches all local addresses in the global VRF.

Examples

The following example shows how to match an IKEv2 policy based on the FVRF and the local IPv4 address:

```
Router(config)# crypto ikev2 policy policy1
Router(config-ikev2-policy)# proposal proposal1
Router(config-ikev2-policy)# match fvrf fvrf1
Router(config-ikev2-policy)# match address local 10.0.0.1
```

The following example shows how to match an IKEv2 policy based on the FVRF and the local IPv6 address:

```
Router(config)# crypto ikev2 policy policy1
Router(config-ikev2-policy)# proposal proposal1
Router(config-ikev2-policy)# match fvrf fvrf1
Router(config-ikev2-policy)# match address local 2001:DB8:0:ABCD::1
```

Related Commands

Command	Description
crypto ikev2 policy	Defines an IKEv2 policy.
proposal	Specifies the proposals that must be used in the IKEv2 policy.
show crypto ikev2 policy	Displays the default or user-defined IKEv2 policy.

match (IKEv2 profile)

To match a profile on front-door VPN routing and forwarding (FVRF) or local parameters such as the IP address, the peer identity, or the peer certificate, use the **match** command in IKEv2 profile configuration mode. To delete a match, use the **no** form of this command.

match {**address local** {*ipv4-address* | *ipv6-address* | **interface** *name*} | **certificate** *certificate-map* | **fvrf** {*fvrf-name* | **any**} | **identity remote** {**address** {*ipv4-address* [*mask*] | *ipv6-address prefix*} | **email** [*domain*] *string* | **fqdn** [*domain*] *string* | **key-id** *opaque-string*}

no match {**address local** {*ipv4-address* | *ipv6-address* | **interface** *name*} | **certificate** *certificate-map*} | **fvrf** {*fvrf-name* | **any**} | **identity remote** {**address** {*ipv4-address* [*mask*] | *ipv6-address prefix*} | **email** [*domain*] *string* | **fqdn** [*domain*] *string* | **key-id** *opaque-string*}

Syntax Description

address local {*ipv4-address* | *ipv6-address*}	Matches the profile based on the local IPv4 or IPv6 address.
interface *name*	Matches the profile based on the local interface.
certificate *certificate-map*	Matches the profile based on fields in the certificate received from the peer.
fvrf *fvrf-name*	Matches the profile based on the user-defined FVRF. The default FVRF is global.
any	Matches the profile based on any FVRF. **Note** The **match vrf any** command must be explicitly configured to match all VRFs.
identity remote	Match a profile based on the remote IKEv2 identity field in the AUTH exchange.
address {*ipv4-address* [*mask*] | *ipv6-address prefix*}	Matches a profile based on the identity of the type remote IPv4 address and its subnet mask or IPv6 address and its prefix length.
key-id *opaque-string*	Matches a profile based on the identity of the type remote key ID.
email	Matches a profile based on the identity of the type remote email ID.
fqdn *fqdn-name*	Matches a profile based on the identity of the type remote Fully Qualified Domain Name (FQDN).
domain *string*	Matches a profile based on the domain part of remote identities of the type FQDN or email.

Command Default

A match is not specified.

Command Modes

IKEv2 profile configuration (crypto-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. Support was added for IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

In an IKEv2 profile, multiple match statements of the same type are logically ORed and match statements of different types are logically ANDed.

Note The **match identity remote** and **match certificate** statements are considered the same type of statements and are ORed.

The result of configuring multiple **match certificate** statements is the same as configuring one **match certificate** statement. Hence, using a single **match certificate** statement as a certificate map caters to multiple certificates and is independent of trustpoints.

Note There can only be one match FVRF statement.

For example, the following command translates to the subsequent “and”, “or” statement:

```
crypto ikev2 profile profile-1
 match vrf green
 match local address 10.0.0.1
 match local address 10.0.0.2
 match certificate remote CertMap
```

(vrf = green AND (local addr = 10.0.0.1 OR local addr = 10.0.0.1) AND remote certificate match CertMap).

There is no precedence between match statements of different types, and selection is based on the first match. Configuration of overlapping profiles is considered as a misconfiguration.

Examples

The following examples show how an IKEv2 profile is matched on the remote identity. The following profile caters to peers that identify using **fqdn example.com** and authenticate with **rsa-signature** using **trustpoint-remote**. The local node authenticates with **pre-share** using **keyring-1**.

```
Router(config)# crypto ikev2 profile profile2
Router(config-ikev2-profile)# match identity remote fqdn example.com
Router(config-ikev2-profile)# identity local email router2@example.com
Router(config-ikev2-profile)# authentication local pre-share
Router(config-ikev2-profile)# authentication remote rsa-sig
Router(config-ikev2-profile)# keyring keyring-1
Router(config-ikev2-profile)# pki trustpoint trustpoint-remote verify
Router(config-ikev2-profile)# lifetime 300
Router(config-ikev2-profile)# dpd 5 10 on-demand
Router(config-ikev2-profile)# virtual-template 1
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.
identity (IKEv2 profile)	Specifies how the local or remote router identifies itself to the peer and communicates with the peer in the RSA authentication exchange.
authentication (IKEv2 profile)	Specifies the local and remote authentication methods in an IKEv2 profile.
keyring (IKEv2 profile)	Specifies a locally defined or AAA-based keyring.
pki trustpoint	Specifies the router to use the PKI trustpoints in the RSA signature authentication.

match invalid-command

To locate invalid commands on a Post Office Protocol, Version 3 (POP 3) server or an Internet Message Access Protocol (IMAP) connection, use the **match invalid-command** in class-map configuration mode. To stop locating invalid commands, use the **no** form of this command.

match invalid-command

no match invalid-command

Syntax Description

This command has no arguments or keywords.

Command Default

It is not required that invalid commands be located.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use this command only after entering the **class-map type inspect imap** or **class-map type inspect pop3** command.

Examples

The following example causes the Zone-Based Policy Firewall software to locate invalid commands on the POP3 server:

```
class-map type inspect pop3 pop3-class
 match invalid-command
```

Related Commands

Command	Description
class-map type inspect imap	Configures inspection parameters for IMAP.
class-map type inspect pop3	Configures inspection parameters for POP3.

match login clear-text

To find a nonsecure login when using an Internet Message Access Protocol (IMAP) or Post Office Protocol, Version 3 (POP3) server, use the **match login clear-text** command in class-map configuration mode. To disable this match criteria, use the **no** form of this command.

match login clear-text

no match login clear-text

Syntax Description

This command has no arguments or keywords.

Command Default

Finding non-secure logins is not required.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use this command either when you are configuring a POP3 firewall class map after you enter the **class-map type inspect pop3** command or when you are configuring an IMAP firewall class map after you enter the **class-map type inspect imap** command.

Examples

The following example determines if the login process is happening in clear-text:

```
class-map type inspect pop3 pop3-class
 match login clear-text
```

Related Commands

Command	Description
class-map type inspect imap	Configures inspection parameters for IMAP.
class-map type inspect pop3	Configures inspection parameters for POP3.
ip inspect name	Defines a set of inspection rules.

match message

To configure the match criterion for a class map on the basis of H.323 protocol messages, use the **match message** command in class-map configuration mode. To remove the H.323-based match criterion from a class map, use the **no** form of this command.

match message *message-name*

no match message *message-name*

Syntax Description

message-name	Name of the message used as a message criterion. The supported message criteria are as follows: • **alerting**—H.225 ALERTING message • **call-proceeding**—H.225 CALL PROCEEDING message • **connect**—H.225 CONNECT message • **facility**—H.225 FACILITY message • **release-complete**—H.225 RELEASE COMPLETE message • **setup**—H.225 SETUP message • **status**—H.225 STATUS message • **status-enquiry**—H.225 STATUS ENQUIRY message

Command Default

None

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Use the **match message** command to inspect H.323 traffic based on the message criterion.

The **match message** command is available under the **class-map type inspect h323** command.

Examples

The following example shows how to configure an H.323 specific class-map to match H.225 SETUP or H.225 RELEASE COMPLETE messages only.

```
class-map type inspect h323 match-any my_h323_rt_msgs
match message setup
match message release-complete
```

Related Commands

Command	Description
class-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect type class map.

match mime content-type regex

To specify Multipurpose Internet Mail Extension (MIME) content file types, which are restricted in attachments in the body of the e-mail being sent over SMTP, use the **match mime content-type regex** command in class-map configuration mode. To disable this inspection parameter, use the **no** form of this command.

match mime content-type regex *content-type-regex*

no match mime content-type regex *content-type-regex*

Syntax Description

content-type-regex	Specifies the type of content in the MIME header in regular expression form.

Command Default

The content type regular expression is not defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

The format of data being transmitted through SMTP is specified by using the MIME standard, which uses headers to specify the content-type, encoding and the filenames of data being sent (text, html, images, applications, documents etc.). The following is an example of an e-mail using the MIME format:

```
From: "foo" <foo@cisco.com>
To: bar <bar@abc.com>
Subject: testmail
Date: Sat, 7 Jan 2006 20:18:47 -0400
Message-ID: <000dadf7453e$bee1bb00$8a22f340@oemcomputer>
MIME-Version: 1.0
Content-Type: image/jpeg;
name='picture.jpg'
Content-Transfer-Encoding: base64
<base64 encoded data for the picture.jpg image>
```

In the above example, the “name=’picture.jpg’” is optional. Even without the definition, the image is sent to the recipient. The e-mail client of the recipient may display it as “part-1”, “attach-1” or it may render the image in-line. Also, attachments are not ‘stripped’ from the e-mail. If a content-type for which ‘reset’ action was configured is detected, an 5XX error code is sent and the connection is closed, in order to prevent the whole e-mail from being delivered. However, the remainder of the e-mail message is sent.

Examples

The following example shows how to configure an SMTP application firewall policy to specify that any form of JPEG image content be restricted in attachments in the body of the e-mail being sent over SMTP:

```
parameter-map type regex jpeg
 pattern "*image//*"

class-map type inspect smtp c1
 match mime content-type regex jpeg

policy-map type inspect smtp p1
 class type inspect smtp c1
 log
```

Related Commands

Command	Description
class-map type inspect smtp	Creates a class map for the SMTP protocol so that the match criteria is set to match criteria for this class map.
class type inspect smtp	Configures an SMTP class-map firewall for SMTP inspection parameters.
parameter-map type regex	Enters the parameter-map name of a specific traffic pattern.
pattern	Cisco IOS regular expression (regex) pattern that matches the traffic pattern for the e-mail sender or user accounts from suspected domains that are causing the spam e-mail.
policy-map type inspect smtp	Create a Layer 7 SMTP policy map.

match mime encoding

To restrict unknown Multipurpose Internet Mail Extension (MIME) content-encoding types or values from being transmitted over SMTP, use the **match mime encoding** command in class-map configuration mode. To disable this inspection parameter, use the **no** form of this command.

match mime encoding {**unknown** | *WORD* | *encoding-type*}

no match mime encoding {**unknown** | *WORD* | *encoding-type*}

Syntax Description

unknown	Specify this keyword if the content-transfer-encoding value in the e-mail does not match any of the ones in the list to restrict unknown and potentially dangerous encodings.
WORD	Specifies a user-defined content-transfer encoding type, which must begin with 'X' (example, "Xmyencodingscheme"). Non-alphanumeric characters, such as hyphens, are not supported.
encoding-type	Specifies one of the pre-configured content-transfer-encoding type: – **7-bit**–ASCII characters – **8-bit**–Facilitates the exchange of e-mail messages containing octets outside the 7-bit ASCII range. – **base64**–Any similar encoding scheme that encodes binary data by treating it numerically and translating it into a base 64 representation. – **quoted-printable**–Encoding using printable characters (i.e. alphanumeric and the equals sign "=") to transmit 8-bit data over a 7-bit data path. It is defined as a MIME content transfer encoding for use in Internet e-mail. – **binary**–Representation for numbers using only two digits (usually, 0 and 1). – **x-uuencode**–Nonstandard encoding. • The **quoted-printable** and **base64** encoding types tell the email client that a binary-to-text encoding scheme was used and that appropriate initial decoding is necessary before the message can be read with its original encoding.

Command Default

The MIME encoding type or value is not defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

The pre-configured content-transfer-encoding types act as a filter on the 'content-transfer-encoding' field in the MIME header within the SMTP body. The 'uuencode' encoding type is not recognized as a standard type by the MIME RFCs because many subtle differences exist in its various implementations. However, since it is used by some mail systems, the **x-uuencode** type is included in the pre-configured list.

Examples

The following example shows how to configure an SMTP application firewall policy to specify that any quoted-printable encoding field in the MIME header within the SMTP body be restricted in e-mail being sent over SMTP:

```
class-map type inspect smtp c1
 match mime encoding quoted-printable

policy-map type inspect smtp p1
 class type inspect smtp c1
 log
```

Related Commands

Command	Description
class-map type inspect smtp	Creates a class map for the SMTP protocol so that the match criteria is set to match criteria for this class map.
class type inspect smtp	Configures an SMTP class-map firewall for SMTP inspection parameters.
log	Generates a log of messages.
policy-map type inspect smtp	Create a Layer 7 SMTP policy map.

match program-number

To specify the allowed Remote Procedure Call (RPC) protocol program number as a match criterion, use the **match program-number** command in class-map configuration mode. To disable this match criterion, use the **no** form of this command.

match program-number *program-number*

no match program-number *program-number*

Syntax Description

program-number	Allowed program number.

Command Default

Disabled

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This match criterion is allowed only for SUN Remote Procedure Call (SUNRPC) class maps. You can use the **match program-number** command only after specifying the **class-map type inspect sunrpc** command.

Examples

The following example configures the program number 2345 as a match criterion in the class map rpc-prog-nums:

```
class-map type inspect sunrpc rpc-prog-nums
 match program-number 2345
```

Related Commands

Command	Description
class-map type inspect sunrpc	Configures inspection parameters for SUNRPC.
ip inspect name	Defines a set of inspection rules.

match protocol (zone)

To configure the match criterion for a class map on the basis of the specified protocol, use the **match protocol** command in class-map configuration mode. To remove the protocol-based match criterion from a class map, use the **no** form of this command.

match protocol *protocol-name* [*parameter-map*] [**signature**]

no match protocol *protocol-name* [*parameter-map*] [**signature**]

Syntax Description

protocol-name	Name of the protocol used as a matching criterion. For a list of supported protocols, use the CLI help option (**?**) on your platform.
parameter-map	(Optional) Protocol-specific parameter map.
signature	(Optional) Enables signature-based classification for peer-to-peer (P2P) packets. **Note** This option is available only for P2P traffic.

Command Default

No protocol-based match criterion for a class map is configured.

Command Modes

class-map configuration (config-cmap)

Command History

Release	Modification
12.4(6)T	This command was introduced for the zone-based policy firewall.
12.4(9)T	This command was modified. Support for the following protocols was added: • P2P protocols: **bittorrent**, **directconnect**, **edonkey**, **fasttrack**, **gnutella**, **kazaa2**, and **winmx** • Instant Messenger (IM) protocols: **aol**, **msnmsgr**, and **ymsgr** Also, the **signature** keyword was added to be used only with P2P protocols.
12.4(11)T	This command was modified. Support for the H.225 Remote Access Services (RAS) protocol and the **h225ras** keyword was added.
12.4(20)T	This command was modified. Support for the I Seek You (ICQ) and Windows Messenger IM protocols and the following keywords was added: **icq**, **winmsgr** Support for the H.323 protocol and the **h323** keyword was added. Support for the Session Initiation Protocol (SIP) protocol and the **sip** keyword was added.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.

Release	Modification
15.0(1)M	This command was modified. The **extended** keyword was removed from the protocol name.
15.1(1)T	This command was modified. Support for the CU-SeeMe protocol and **cuseeme** keyword was removed.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S. The following keywords were added: **netbios-dgm**, **netbios-ns**, and **netbios-ssn**.

Usage Guidelines

Use the **match protocol** command to specify the traffic based on a particular protocol. You can use this command in conjunction with the **match access-group** and **match class-map** commands to build sophisticated traffic classes.

The **match protocol** command is available under the **class-map type inspect** command.

If you enter the **match protocol** command under the **class-map type inspect** command, the Port to Application Mappings (PAM) are honored when the protocol field in the packet is matched against this command. All the port mappings configured in the PAM table appear under the class map.

When packets are matched to a protocol, a traffic rate is generated for these packets. In a zone-based firewall policy, only the first packet that creates a session matches the policy. Subsequent packets in this flow do not match the filters in the configured policy, but instead match the session directly. The statistics related to subsequent packets are shown as part of the inspect action.

In Cisco IOS Release 12.4(15)T only, if Simple Mail Transfer Protocol (SMTP) is currently configured for inspection in a class map and the inspection of Extended SMTP (ESMTP) needs to be configured, then the **no match protocol smtp** command must be entered before adding the **match protocol smtp extended** command. To revert to regular SMTP inspection, use the **no match protocol smtp extended** command and then enter the **match protocol smtp** command.

In Cisco IOS Release 12.4(15)T, if these commands are not configured in the proper order, then the following error displays:

```
%Cannot add this filter.Remove match protocol smtp filter and then add this filter
```

In Cisco IOS Release 15.0(1)M and later releases, the **extended** keyword was removed from the **match protocol smtp** command.

Examples

The following example shows how to specify a class map called c1 and configure the HTTP protocol as a match criterion:

```
class-map type inspect c1
 match protocol http
```

The following example shows how to specify different class maps for ICQ and Windows Messenger IM applications:

```
! Define the servers for ICQ.
parameter-map type protocol-info icq-servers
 server name *.icq.com snoop
 server name oam-d09a.blue.aol.com

! Define the servers for Windows Messenger.
parameter-map type protocol-info winmsgr-servers
 server name messenger.msn.com snoop
```

```
! Define servers for yahoo.
parameter-map type protocol-info yahoo-servers
 server name scs*.msg.yahoo.com snoop
 server name c*.msg.yahoo.com snoop

! Define class-map to match ICQ traffic.
class-map type inspect icq-traffic
 match protocol icq icq-servers

! Define class-map to match windows Messenger traffic.
class-map type inspect winmsgr-traffic
 match protocol winmsgr winmsgr-servers
!

! Define class-map to match text-chat for windows messenger.
class-map type inspect winmsgr winmsgr-textchat
 match service text-chat
!

Define class-map to match default service
class-map type inspect winmsgr winmsgr-defaultservice
 match service any
!
```

The following example shows how to specify a class map called c1 and configure the netbios-dgm protocol as a match criterion:

```
class-map type inspect c1
 match protocol netbios-dgm
```

Related Commands

Command	Description
class-map type inspect	Creates a Layer 3 or Layer 4 inspect type class map.
match access-group	Configures the match criteria for a class map based on the specified ACL.

match protocol h323-annexe

To enable the inspection of H.323 protocol Annex E traffic which works on the User Datagram Protocol (UDP) diagnostic port or TCP port 2517, use the **match protocol h323-annexe** command in class-map configuration mode. To disable the inspection, use the **no** form of this command.

match protocol h323-annexe

no match protocol h323-annexe

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Use the **match protocol h323-annexe** command to inspect traffic based on Annex E of the H.323 protocol that uses the UDP diagnostic port or TCP port 2517. You can use this command in conjunction with the **match access-group** command to build sophisticated traffic classes.

The **match protocol h323-annexe** command is available under the **class-map type inspect** command.

Examples

The following example shows how to configure a voice policy to inspect the H.323 protocol Annex E packets for the “my-voice-class” class map.

```
class-map type inspect match-all my-voice-class
 match protocol h323-annexe
```

Related Commands

Command	Description
class-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect type class map.
match access-group	Configures the match criteria for a class map based on the specified ACL.
match protocol h323-nxg	Enables the inspection of H.323 protocol Annex G traffic exchanged between border elements (BE) using the User Datagram Protocol (UDP) diagnostic port or TCP port 2099.

match protocol h323-nxg

To enable the inspection of H.323 protocol Annex G traffic exchanged between border elements (BE) using User Datagram Protocol (UDP) diagnostic port or TCP port 2099, use the **match protocol h323-nxg** command in class-map configuration mode. To disable the inspection, use the **no** form of this command.

match protocol h323-nxg

no match protocol h323-nxg

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Use the **match protocol h323-nxg** command to inspect traffic based on Annex G of the H.323 protocol that uses the UDP diagnostic port or TCP port 2099 to exchange traffic between border elements. You can use this command in conjunction with the **match access-group** command to build sophisticated traffic classes.

The **match protocol h323-nxg** command is available under the **class-map type inspect** command.

Examples

The following example shows how to configure a voice policy to inspect the H.323 protocol Annex G packets for the “my-voice-class” class map.

```
class-map type inspect match-all my-voice-class
 match protocol h323-nxg
```

Related Commands

Command	Description
class-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect type class map.
match access-group	Configures the match criteria for a class map based on the specified ACL.
match protocol h323-annexe	Enables the inspection of H.323 protocol Annex E traffic which works on the UDP diagnostic port or TCP Port 2517.

match protocol-violation

To configure a Session Initiation Protocol (SIP) class map to use the protocol-violation method as a match criterion for permitting or denying SIP traffic, use the **match protocol-violation** command in class-map configuration mode. To remove the protocol-violation based match criterion from a class map, use the **no** form of this command.

match protocol-violation

no match protocol-violation

Syntax Description

This command has no arguments or keywords.

Command Default

No match criterion is configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command when configuring an SIP firewall class map, after entering the **class-map type inspect** command.

Examples

The following example shows how to specify the protocol-violation method as a match criterion.

```
Router(config)# class-map type inspect sip sip-class
Router(config-cmap)# match protocol-violation
```

Related Commands

Command	Description
class-map type inspect sip	Creates a class map for SIP.

match recipient address regex

To specify a non-existent e-mail recipient pattern in order to learn a spam sender and their domain information by luring them to use this contrived e-mail recipient, use the **match recipient address regex** command in class-map configuration mode. To disable this inspection parameter, use the **no** form of this command.

match recipient address regex *parameter-map-name*

no match recipient address regex *parameter-map-name*

Syntax Description

parameter-map-name	Specifies the name of the non-existent e-mail recipient pattern.

Command Default

The fictitious names of e-mail recipients are not defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

A non-existent e-mail recipient pattern can be specified to learn about a spam sender and their domain information by luring them to use this non-existent e-mail recipient pattern. This pattern is a regular-expression (regex) that can be specified to identify an e-mail addressed to a particular recipient or domain when a server is functioning as a relay. The specified pattern is checked in the SMTP RCPT command (SMTP envelope) parameter to identify if the recipient is either used as an argument or a source-list to forward mail in the route specified in the list.

Note The **match recipient address regex** command does not operate on the ‘To’ or ‘Cc’ fields in the e-mail header.

Examples

The following example shows how to configure a regular expression non-existent e-mail recipient pattern:

```
parameter-map type regex known-unknown-users
 pattern "john@mydomain.com"

class-map type inspect smtp c1
 match recipient address regex known-unknown-users

policy-map type inspect smtp p1
 class type inspect smtp c1
 reset
```

Related Commands

Command	Description
class-map type inspect smtp	Creates a class map for the SMTP protocol so that the match criteria is set to match criteria for this class map.
class type inspect smtp	Configures an SMTP class-map firewall for SMTP inspection parameters.
parameter-map type regex	Enters the parameter-map name of a specific traffic pattern.
pattern	Cisco IOS regular expression (regex) pattern that matches the traffic pattern for the e-mail sender or user accounts from suspected domains that are causing the spam e-mail.
policy-map type inspect smtp	Create a Layer 7 SMTP policy map.
reset	(Optional) Drops an SMTP connection with an SMTP sender (client) if it violates the specified policy. This action sends an error code to the sender and closes the connection gracefully.

match recipient count gt

To specify an action that occurs when a number of invalid recipients appear on an SMTP connection, use the **match recipient count gt** command in class-map configuration mode. To disable this inspection parameter, use the **no** form of this command.

match recipient count gt *value*

no match recipient count gt *value*

Syntax Description

value	Specifies the number of RCPT SMTP commands sent by the sender (client) to recipients who are specified in a single SMTP transaction to limit these commands.

Command Default

The number of RCPT SMTP commands sent by a sender to recipients is not defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

Spammers who search for a large number of user accounts in a domain typically send the same e-mail to all the user accounts they find in this domain. Spammers can be identified and restricted from searching for user accounts in a domain by using the **match recipient count gt** command.

Note The **match recipient count gt** command does not count the number of recipients specified in the 'To:' or 'Cc:' fields in the e-mail header.

Examples

The following example shows how to configure an SMTP application firewall policy to determine the number of **RCPT** lines and invalid recipients, for which the server has replied "500 No such address," in the SMTP transaction:

```
class-map type inspect smtp c1
 match recipient count gt 25

policy-map type inspect smtp p1
 class type inspect smtp c1
 reset
```

Related Commands

Command	Description
class-map type inspect smtp	Creates a class map for the SMTP protocol so that the match criteria is set to match criteria for this class map.
class type inspect smtp	Configures an SMTP class-map firewall for SMTP inspection parameters.
policy-map type inspect smtp	Create a Layer 7 SMTP policy map.
reset	(Optional) Drops an SMTP connection with an SMTP sender (client) if it violates the specified policy. This action sends an error code to the sender and closes the connection gracefully.

match recipient invalid count gt

To identify and restrict the number of invalid SMTP recipients that can appear in an e-mail from senders who try common names on a domain in the hope that they discover a valid user name to whom they can send spam, use the **match recipient invalid count gt** command in class-map configuration mode. To disable this inspection parameter, use the **no** form of this command.

match recipient invalid count gt *value*

no match sender address regex *value*

Syntax Description

value	Specifies a maximum number of invalid e-mail recipients on this SMTP connection.

Command Default

The a number of invalid e-mail recipients is not defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

If a sender specifies in an invalid e-mail recipient and SMTP encounters this invalid recipient on the SMTP connection, then SMTP sends an error code reply to the e-mail sender (client) to specify another recipient. In this case, the event did not violate the SMTP protocol or indicate that this particular SMTP connection is bad. However, if a pattern of invalid recipients appears, then a reasonable threshold can be set to restrict these nuisance SMTP connections.

Examples

The following example shows how to configure an SMTP application firewall policy that restricts the number of invalid e-mail recipients on this SMTP connection to 5:

```
class-map type inspect smtp c1
 match recipient invalid count gt 5

policy-map type inspect smtp p1
 class type inspect smtp c1
 reset
```

Related Commands

Command	Description
class-map type inspect smtp	Creates a class map for the SMTP protocol so that the match criteria is set to match criteria for this class map.
class type inspect smtp	Configures an SMTP class-map firewall for SMTP inspection parameters.
policy-map type inspect smtp	Create a Layer 7 SMTP policy map.
reset	(Optional) Drops an SMTP connection with an SMTP sender (client) if it violates the specified policy. This action sends an error code to the sender and closes the connection gracefully.

match reply ehlo

To identify and mask a service extension parameter in the EHLO server reply (e.g. 8BITMIME, ETRN) to prevent a sender (client) from using that particular service extension, use the **match reply ehlo** command in class-map configuration mode. To disable this inspection parameter, use the **no** form of this command.

match reply ehlo {*parameter* | *WORD*}

no match reply ehlo {*parameter* | *WORD*}

Syntax Description

parameter	Specify a parameter from the well-known EHLO keywords.
WORD	Specify an extension which is not on the EHLO list (e.g. private extension XFOOBAR). Non-alphanumeric characters, such as hyphens, are not supported.

Command Default

The service extension parameter in the EHLO server reply is not defined or masked.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Examples

The following example shows how to configure an SMTP application firewall policy that identifies and masks a well-known service extension parameter in the EHLO server reply:

```
class-map type inspect smtp c1
 match reply ehlo ETRN

policy-map type inspect smtp p1
 class type inspect smtp c1
 log
 mask
```

Related Commands

Command	Description
class-map type inspect smtp	Creates a class map for the SMTP protocol so that the match criteria is set to match criteria for this class map.
class type inspect smtp	Configures an SMTP class-map firewall for SMTP inspection parameters.
log	Logs an action related to this class-type in the SMTP policy map.

Command	Description
mask (policy-map)	Explicitly masks specified SMTP commands or the parameters returned by the server in response to an EHLO command.
policy-map type inspect smtp	Create a Layer 7 SMTP policy map.

match req-resp

To configure a Session Initiation Protocol (SIP) class map to use the req-resp methods as a match criterion for permitting or denying SIP traffic, use the **match req-resp** command in class-map configuration mode. To remove the req-resp based match criterion from a class map, use the **no** form of this command.

match req-resp header *field* **regex** *regex-parameter-map*

no match req-resp header *field* **regex** *regex-parameter-map*

Syntax Description

header	Identifies the SIP header field.
field	Name of the request header field. The following are valid request header fields: **accept**, **accept-encoding**, **accept-language**, **alert-info**, **allow**, **contact**, **content-disposition**, **content-encoding**, **content-language**, **content-length**, **content-type**, **from**, **record-route**, **supported**, **to**, **user-agent**, **via**.
regex	Indicates that a regular expression will follow.
regex-parameter-map	Configures a parameter map of type **regex**.

Command Default

No match criterion is configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command when configuring an SIP firewall class map, after entering the **class-map type inspect** command.

Examples

The following example shows how to specify the req-resp method as a match criterion.

```
Router(config)# class-map type inspect sip sip-class
Router(config-cmap)# match req-resp header via regex unsecure_proxy
```

Related Commands

Command	Description
class-map type inspect sip	Creates a class map for SIP.

match req-resp body length

To configure an HTTP class map to use the minimum or maximum message size, in bytes, as a match criterion for permitting or denying HTTP traffic through the firewall, use the **match req-resp body length** command in class-map configuration mode. To remove message-size limitations from your configuration, use the **no** form of this command.

match req-resp body length {**lt** *bytes* | **gt** *bytes*}

no match req-resp body length {**lt** *bytes* | **gt** *bytes*}

Syntax Description

lt *bytes*	Minimum number of bytes in each message. The range is from 0 to 65535.
gt *bytes*	Message cannot be greater than the specified number of bytes.

Command Default

Message size is not considered when permitting or denying HTTP messages.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use this command when you are configuring an HTTP firewall policy map,only after entering the **class-map type inspect http** command.

If the message body length is less than or greater than the specified values, a match occurs.

Examples

The following example, which shows how to define the HTTP application firewall policy http-class, will not permit HTTP messages longer than 1 byte:

```
class-map type inspect http http-class
 match req-resp body length 1
```

Related Commands

Command	Description
class-map type inspect http	Creates a class map for HTTP.

match req-resp header content-type

To match traffic based on the content type of the HTTP body, use the **match req-resp header content-type** command in class-map configuration mode. To disable this inspection parameter, use the **no** form of this command.

match req-resp header content-type {**violation** | **mismatch** | **unknown**}

no match req-resp header content-type {**violation** | **mismatch** | **unknown**}

Syntax Description

violation	Flags a match if the content-type definition and the content type of the actual body do not match.
mismatch	Verifies the content-type of the response message against the accept field value of the request message.
unknown	Flags a match when an unknown content-type is found.

Command Default

No content-type checking is performed.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use the **match req-resp header content-type** command when you are configuring an HTTP firewall policy map, only after entering the **class-map type inspect http** command.

The **match req-resp header content-type** command configures a policy based on the content type of HTTP traffic. The command verifies that the header is one of the following supported content types:

- audio/*
- audio/basic
- audio/midi
- audio/mpeg
- audio/x-adpcm
- audio/x-aiff
- audio/x-ogg
- audio/x-wav
- application/msword
- application/octet-stream
- application/pdf
- application/postscript

- application/vnd.ms-excel
- application/vnd.ms-powerpoint
- application/x-gzip
- application/x-java-arching
- application/x-java-xm
- application/zip
- image/*
- image/cgf
- image/gif
- image/jpeg
- image/png
- image/tiff
- image/x-3ds
- image/x-bitmap
- image/x-niff
- image/x-portable-bitmap
- image/x-portable-greymap
- image/x-xpm
- text/*
- text/css
- text/html
- text/plain
- text/richtext
- text/sgml
- text/xmcd
- text/xml
- video/*
- video/-flc
- video/mpeg
- video/quicktime
- video/sgi
- video/x-avi
- video/x-fli
- video/x-mng
- video/x-msvideo

Examples

The following example configures an HTTP class map based on the content type of HTTP traffic:

```
class-map type inspect http http-class
 match req-resp header content-type unknown
```

Related Commands

Command	Description
class-map type inspect http	Creates a class map for HTTP.
content-type-verification	Permits or denies HTTP traffic through the firewall on the basis of content message type.
content-type-verification-match-req-rsp	Verifies the content type of the HTTP response against the accept field of the HTTP request.

match req-resp header transfer-encoding

To permit or deny HTTP traffic according to the specified transfer encoding of the message, use the **match req-resp header transfer-encoding** command in class-map configuration mode. To remove this match criterion, use the **no** form of this command.

match req-resp header transfer-encoding {**chunked** | **compress** | **deflate** | **gzip** | **identity** | **all**}

no match req-resp header transfer-encoding {**chunked** | **compress** | **deflate** | **gzip** | **identity** | **all**}

Syntax Description

chunked	Encoding format (specified in RFC 2616, Hypertext Transfer Protocol—HTTP/1) in which the body of the message is transferred in a series of chunks; each chunk contains its own size indicator.
compress	Encoding format produced by the UNIX compress utility.
deflate	ZLIB format defined in RFC 1950, ZLIB Compressed Data Format Specification Version 3.3, combined with the deflate compression mechanism described in RFC 1951, DEFLATE Compressed Data Format Specification Version 1.3.
gzip	Encoding format produced by the gzip (GNU zip) program.
identity	Default encoding, which indicates that no encoding has been performed.
all	All of the transfer encoding types.

Command Default

None

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use this command when you are configuring an HTTP firewall policy map, after entering the **class-map type inspect http** command.

Examples

The following example permits or denies HTTP traffic according to the encoding format produced by the UNIX compress utility:

```
class-map type inspect http http-class
 match req-resp header transfer-encoding compress
```

Related Commands

Command	Description
class-map type inspect http	Creates a class map for HTTP.
transfer-encoding type	Permits or denies HTTP traffic according to the specified transfer-encoding of the message.

match req-resp protocol-violation

To allow HTTP messages to pass through the firewall or to reset the TCP connection when HTTP noncompliant traffic is detected, use the **match req-resp protocol-violation** command in class-map configuration mode. To disable configured settings, use the **no** form of this command.

match req-resp protocol-violation

no match req-resp protocol-violation

Syntax Description

This command has no arguments or keywords.

Command Default

All traffic is allowed through the firewall.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use this command when you are configuring an HTTP firewall policy map, after entering the **class-map type inspect http** command.

The **match req-resp protocol-violation** command allows HTTP messages to pass through the firewall, If desired, in the policy map you can reset the TCP connection when HTTP noncompliant traffic is detected.

Examples

The following example allows HTTP messages to pass through the firewall:

```
class-map type inspect http http-class
 match req-resp protocol-violation
```

Related Commands

Command	Description
class-map type inspect http	Creates a class map for HTTP.

match request

To configure a Session Initiation Protocol (SIP) class map to use the request methods as a match criterion for permitting or denying SIP traffic, use the **match request** command in class-map configuration mode. To remove request based match criterion from a class map, use the **no** form of this command.

match request {**method** *method-name* | **header** *field* **regex** *regex-parameter-map*}

no match request {**method** *method-name* | **header** *field* **regex** *regex-parameter-map*}

Syntax Description

method	Identifies the SIP request method.
method-name	Name of the method (for example, **ack**) used as a matching criterion. See the "Usage Guidelines" for a list of methods supported by most routers.
header	Identifies the SIP header field.
field	Name of the request header field. The following are valid request header fields: **accept**, **accept-encoding**, **accept-language**, **alert-info**, **allow**, **authorization**, **contact**, **content-disposition**, **content-encoding**, **content-language**, **content-length**, **content-type**, **from**, **in-reply-to**, **max-forwards**, **priority**, **proxy-authorization**, **proxy-require**, **record-route**, **route**, **subject**, **supported**, **to**, **user-agent**, **via**, **warning**.
regex	Indicates that a regular expression will follow.
regex-parameter-map	Configures a parameter map of type **regex**.

Command Default

No match criterion is configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command when configuring an SIP firewall class map, after entering the **class-map type inspect** command.

Supported Methods

Table 42 lists the request methods supported by most routers. For a complete list of supported methods, see the online help for the **match request** command on the router that you are using.

Table 42 Supported Methods

Method Name	Description
ack	Acknowledges that the previous message is valid and accepted.
bye	Signifies intent to terminate a call.
cancel	Terminates any pending request.
info	Communicates midsession signaling information along the signaling path for a call.
invite	Sets up a call.
message	Sends an instant message.
notify	Informs subscribers of state changes.
options	Allows a user-agent (UA) to query another UA or a proxy server about its capabilities.
prack	Provides reliable transfer of provisional response messages.
refer	Indicates that the recipient should contact a third party using the contact information provided in the request.
register	Includes a contact address to which SIP requests for the address-of-record should be forwarded.
subscribe	Requests state subscription. It is a dialog creating method.
update	Allows a client to update the parameters of a session (for example, the set of media streams and their codecs), but has no impact on the state of a dialog.

Examples

The following example shows how to specify the request method **subscribe** as a match criterion.

```
Router(config)# class-map type inspect sip sip-class
Router(config-cmap)# match request method subscribe
```

Related Commands

Command	Description
class-map type inspect sip	Creates a class map for SIP.

match request length

To configure an HTTP firewall policy to use the uniform resource identifier (URI) or argument length in the request message as a match criterion for permitting or denying HTTP traffic, use the **match request length** command in class-map configuration mode. To remove this match criterion, use the **no** form of this command.

match request {**uri** | **arg**} **length gt** *bytes*

no match request {**uri** | **arg**} **length gt** *bytes*

Syntax Description

uri | **arg**	Firewall will search the URI or argument length of the request message as the match criterion.
gt *bytes*	Permits HTTP traffic if the URL in the request message contains more than the specified number of bytes.

Command Default

URI or argument lengths are not considered when permitting or denying HTTP traffic.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(9)T	The **arg** keyword was added.

Usage Guidelines

Use the **match request length** command to verify the length of the URI or argument that is being sent in a request message and apply the configured action when the length exceeds the configured threshold.

If a match is found, possible actions that can be specified within the policy are as follows: allow, reset, or log. (The log action triggers a syslog message when a match is found.)

Examples

The following example shows how to configure an HTTP application firewall policy to raise an alarm whenever the URI length of a request message exceeds 3076 bytes:

```
class-map type inspect http uri_len_cm
 match request uri length gt 3076

policy-map type inspect http uri_len_pm
 class type inspect http uri_len_cm
 log
```

The following example shows how to configure an HTTP application firewall policy to raise an alarm whenever the argument length of a request message exceeds 512 bytes.

```
class-map type inspect http arg_len_cm
 match request arg length gt 512

policy-map type inspect http arg_len_pm
 class type inspect http arg_len_cm
 log
```

match request method

To configure an HTTP class map to use the request methods or the extension methods as a match criterion for permitting or denying HTTP traffic, use the **match request method** command in class-map configuration mode. To remove this match criterion, use the **no** form of this command.

match request method {**connect** | **copy** | **delete** | **edit** | **get** | **getattribute** | **getattributenames** | **getproperties** | **head** | **index** | **lock** | **mkdir** | **move** | **options** | **post** | **put** | **revadd** | **revlabel** | **revlog** | **revnum** | **save** | **setattribute** | **startrev** | **stoprev** | **trace** | **unedit** | **unlock**}

no match request method {**connect** | **copy** | **delete** | **edit** | **get** | **getattribute** | **getattributenames** | **getproperties** | **head** | **index** | **lock** | **mkdir** | **move** | **options** | **post** | **put** | **revadd** | **revlabel** | **revlog** | **revnum** | **save** | **setattribute** | **startrev** | **stoprev** | **trace** | **unedit** | **unlock**}

Syntax Description

connect	Connect method.
copy	Copy extension method.
delete	Delete method.
edit	Edit extension method.
get	Get method.
getattribute	Getattribute extension method.
getattributenames	Getattributenames extension method.
getproperties	Getproperties method.
head	Head method.
index	Index extension method.
lock	Lock extension method.
mkdir	Mkdir extension method.
move	Move extension method.
options	Options method.
post	Post method.
put	Put method.
revadd	Revadd extension method.
revlabel	Revlabel extension method.
revlog	Revlog extension method.
revnum	Revnum extension method.
save	Save extension method.
setattribute	Setattribute extension method.
startrev	Startrev extension method.
stoprev	Stoprev extension method.
trace	Trace method.
unedit	Unedit extension method.
unlock	Unlock extension method.

Command Default None

Command Modes Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines You can use this command when you are configuring an HTTP firewall class map, after entering the **class-map type inspect http** command.

Examples The following example specifies that the match criteria is connect:

```
class-map type inspect http http-class
 match request method connect
```

Related Commands

Command	Description
class-map type inspect http	Creates a class map for HTTP.

match request not regex

To negate a match result in a HTTP firewall policy, use the **match request not regex** command in class-map configuration mode. To reset the match criterion, use the **no** form of this command.

match request not uri regex *parameter-map-name*

no match request not uri regex *parameter-map-name*

Syntax Description

uri	Firewall policy will search the URI or argument as the match criterion.
parameter-map-name	HTTP-based parameter map as specified via the **parameter-map type** command.

Command Default

Match negation is not enabled.

Command Modes

Class-map configuration (config-cmap)#

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

Use the **match request not uri regex** command to negate a match result.

Examples

The following example shows how to negate a match result and the output of the configuration in the running configuration.

```
Router(config)# policy-map type inspect http httppmap
Router(config-cmap)# match not request uri regex pmap
Router(config-cmap)# match request method post
Route(config-pmap)# class type inspect http cmap
Router(config-pmap-c)# reset
Router(config-pmap-c)# log
```

In the following configuration, if the HTTP POST request does not match the URL regular expression, It will be classified under class “httpcmap” and firewall will RESET the connection as it has RESET configured for this class.

```
parameter-map type regex pmap
 pattern .*Publications/OrderHardcopies/tabid/123/Default.aspx

class-map type inspect http match-all httpcmap
 match not request uri regex pmap
 match request method post

policy-map type inspect http pmap
 class type inspect http httpcmap
   reset
   log
```

```
class class-default
```

Related Commands

Command	Description
parameter-map type	Defines a parameter map.
class-map type inspect	Defines an inspect type class map.
match request regex	Defines a HTTP firewall policy to permit or deny HTTP traffic.
policy-map type inspect	Defines an inspect type policy map.

match request port-misuse

To identify applications misusing HTTP port, use the **match request port-misuse** command in class-map configuration mode. To remove this inspection parameter, use the **no** form of this command.

match request port-misuse {**im** | **p2p** | **tunneling** | **any**}

no match request port-misuse {**im** | **p2p** | **tunneling** | **any**}

Syntax Description

im	Instant messaging protocol applications subject to inspection.
p2p	Peer-to-peer protocol applications subject to inspection.
tunneling	Tunneling applications subject to inspection: HTTPPort/HTTPHost.
any	Any type of misuse (**im**, **p2p**, and **tunneling**).

Command Default

Applications that are misusing the HTTP port cannot be identified.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use this command only after entering the **class-map type inspect http** command.

Examples

The following example identifies all types of misuse of the HTTP port:

```
class-map type inspect http http-class
 match request port-misuse any
```

Related Commands

Command	Description
class-map type inspect http	Creates a class map for HTTP.
port-misuse	Permits or denies HTTP traffic through the firewall on the basis of specified applications in the HTTP message.

match request regex

To configure an HTTP firewall policy to permit or deny HTTP traffic on the basis of request messages whose uniform resource identifier (URI) or arguments (parameters) match a defined regular expression, use the **match request regex** command in class-map configuration mode. To remove this match criterion, use the **no** form of this command.

match request {**uri** | **arÅg**} **regex** *parameter-map-name*

no match request {**uri** | **arg**} **regex** *parameter-map-name*

Syntax Description

uri | **arg**	Firewall policy will search the URI or argument as the match criterion.
parameter-map-name	HTTP-based parameter map as specified via the **parameter-map type** command.

Command Default

URI or parameter matching is not enabled.

Command Modes

Class-map configuration (config-cmap)#

Command History

Release	Modification
12.4(9)T	This command was introduced.
15.1(1)T	The **not** keyword was added.

Usage Guidelines

Use the **match request uri regex** command to block custom URLs and queries; use the **match request arg regex** command to block all messages whose parameters match the configured regular inspection.

If a match is found, possible actions that can be specified within the policy are as follows: allow, reset, or log. (The log action triggers a syslog message when a match is found.)

Examples

The following example shows how to configure an HTTP application firewall policy to block any request whose URI matches any of the following regular expressions: ".*cmd.exe," ".*money," ".*gambling".

```
parameter-map type regex uri_regex_cm
 pattern ".*cmd.exe"
 pattern ".*money"
 pattern ".*gambling"

class-map type inspect http uri_check_cm
 match request uri regex uri_regex_cm

policy-map type inspect http uri_check_pm
 class type inspect http uri_check_cm
 reset
```

The following example shows how to configure an HTTP application firewall policy to block any request whose arguments match the ".*codered" or the ".*attack" regular expressions:

```
parameter-map type regex arg_regex_cm
 pattern ".*codered"
 pattern ".*attack"

class-map type inspect http arg_check_cm
 match request arg regex arg_regex_cm

policy-map type inspect http arg_check_pm
 class type inspect http arg_check_cm
 reset
```

Related Commands

Command	Description
parameter-map type	Defines a parameter map.
class-map type inspect	Defines an inspect type class map.
policy-map type inspect	Defines an inspect type policy map.

match response

To configure a Session Initiation Protocol (SIP) class map to use a response method as the match criterion for permitting or denying SIP traffic, use the **match response** command in class-map configuration mode. To remove the response based match criterion from a class map, use the **no** form of this command.

match response {**header** *field* | **status**} **regex** *regex-parameter-map*

no match response {**header** *field* | **status**} **regex** *regex-parameter-map*

Syntax Description

header	(Optional) Identifies the SIP header field.
field	Name of the request header field. The following are valid request header fields: **accept**, **accept-encoding**, **accept-language**, **alert-info**, **allow**, **authentication-info**, **contact**, **content-disposition**, **content-encoding**, **content-language**, **content-length**, **content-type**, **error-info**, **from**, **proxy-authenticate**, **record-route**, **retry-after**, **server**, **supported**, **to**, **user-agent**, **via**, **www-authenticate**.
status	(Optional) Identifies status line in response.
regex	Indicates that a regular expression will follow.
regex-parameter-map	Name of parameter-map.

Command Default

No match criterion is configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command when configuring an SIP firewall class map, after entering the **class-map type inspect** command.

Examples

The following example shows how to specify the response method as a match criterion.

```
Router(config)# class-map type inspect sip sip-class
Router(config-cmap)# match response status regex allowed-im-users
```

Related Commands

Command	Description
class-map type inspect sip	Creates a class map for SIP.

match response body java-applet

To identify Java applets in an HTTP connection., use the **match response body java-applet** command in class-map configuration mode. To remove this inspection rule, use the **no** form of this command.

match response body java-applet

no match response body java-applet

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use this command when you are configuring an HTTP firewall policy map, after entering the **class-map type inspect http** command.

Examples

The following example identifies Java applets in an HTTP connection:

```
class-map type inspect http http-class
 match response body java-applet
```

Related Commands

Command	Description
class-map type inspect http	Creates a class map for HTTP.
ip inspect name test http java-list	For Java applet blocking, specifies the numbered standard access list to use to determine friendly sites.

match response status-line regex

To specify a list of regular expressions that are to be matched against the status line of a response message, use the **match response status-line regex** command in class-map configuration mode. To remove this match criterion, use the **no** form of this command.

match response status-line regex *parameter-map-name*

no match response status-line regex *parameter-map-name*

Syntax Description

parameter-map-name	Name of parameter map.

Command Default

The status line of response messages is not considered when permitting or denying HTTP traffic.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

If a match is found, possible actions that can be specified within the policy are as follows: allow, reset, or log. (The log action triggers a syslog message when a match is found.)

Examples

The following example shows how to configure an HTTP firewall policy to log an alarm whenever an attempt is made to access a forbidden page. (A forbidden page usually contains a 403 status-code and the status line looks like “HTTP/1.0 403 page forbidden\r\n”.)

```
parameter-map type regex status_line_regex
 pattern "[Hh][Tt][Tt][Pp][/][0-9][.][0-9][ \t]+403"

class-map type inspect http status_line_cm
 match response status-line regex status_line_regex

policy-map type inspect http status_line_pm
 class type inspect http status_line_cm
 log
```

match search-file-name

To use filenames within a search request as the match criterion, use the **match search-file-name** command in class-map configuration mode. To remove this match criterion from the configuration file, use the **no** form of this command.

match search-file-name [*regular-expression*]

no match search-file-name [*regular-expression*]

Syntax Description

regular-expression	(Optional) The regular expression used to identify specific filenames within a search request. For example, entering ".exe" as the regular expression would classify the filenames containing the string ".exe" as matches for the traffic policy. If this argument is not issued, all filenames are classified, as appropriate.

Command Default

None

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Use the **match search-file-name** command to configure the Cisco IOS Firewall to block filenames within a search request for clients using the eDonkey peer-to-peer (P2P) protocol.

Note This command is available only for the eDonkey P2P protocol.

Examples

The following example shows how to configure a Cisco IOS Firewall to block filename searches for ".exe" and permit file transfers within the eDonkey protocol:

```
! Select eDonkey protocol requiring L7 policies
class-map type inspect match-any my-restricted-p2p
 match protocol edonkey signature
!
! Configure Edonkey to look for "*.exe" in searches
class-map type inspect edonkey my-edonkey-exe
 match search-file-name "*.exe"
!
! Configure Edonkey to look for file-transfers
class-map type inspect edonkey my-edonkey-file-tx
 match file-transfer *
!
```

```
! Configure P2P Layer 7 policy map
policy-map type inspect p2p my-p2p-policy
! class type inspect edonkey my-edonkey-exe
 reset
 class type inspect edonkey my-edonkey-file-tx
 allow
 log
!
!
```

Related Commands

Command	Description
class-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect type class map.

match sender address regex

To specify spam e-mail from suspected domains and user accounts to be restricted, use the **match sender address regex** command in class-map configuration mode. To disable this inspection parameter, use the **no** form of this command.

match sender address regex *parameter-map-name*

no match sender address regex *parameter-map-name*

Syntax Description

parameter-map-name	Specifies the parameter-map name class, which is the name of a specific traffic pattern. This pattern is a Cisco IOS regular expression (regex) pattern for a class-map.

Command Default

The parameter-map name class is not defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

The **match sender address regex** command helps to match the parameter-map name of a specific traffic pattern that specifies a sender domain or e-mail address in the SMTP traffic. The specified pattern is scanned in the parameter for the SMTP **MAIL FROM:** command.

Examples

The following example shows how to configure an SMTP application firewall policy to restrict an e-mail sender from a suspected domain:

```
parameter-map type regex bad-guys
 pattern "*deals\.com"
 pattern *crazyperson*@hotmail\.com

class-map type inspect smtp match-any c1
 match sender address regex bad-guys

policy-map type inspect smtp p1
 class type inspect smtp c1
 log
 reset
```

Related Commands

Command	Description
class-map type inspect smtp	Creates a class map for the SMTP protocol so that the match criteria is set to match criteria for this class map.
parameter-map type regex	Enters the parameter-map name of a specific traffic pattern.
pattern	Cisco IOS regular expression (regex) pattern that matches the traffic pattern for the e-mail sender or user accounts from suspected domains that are causing the spam e-mail.

match server-domain urlf-glob

To configure the match criteria for a local URL filtering class map on the basis of server domain name, use the **match server-domain urlf-glob** command in class-map configuration mode. To remove the domain name match criteria from a URL filtering class map, use the **no** form of this command.

match server-domain urlf-glob *parameter-map-name*

no match server-domain urlf-glob *parameter-map-name*

Syntax Description

parameter-map-name	Name of the parameter map.

Command Default

No match criteria are configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **match server-domain urlf-glob** command specifies the server domain matches for local URL filtering. Typically, you use this command in two class maps: one to specify trusted domains and one to specify untrusted domains. You must configure the **urlf-glob** keyword with the **parameter-map type urlf-glob** command and create the local filtering class with the **class-map type urlfilter** command before using this command, otherwise you will receive an error message.

Examples

The following example shows the configuration for trusted domains and untrusted domains:

```
parameter-map type urlf-glob trusted-domain-param
 pattern www.example.com
 pattern *.example1.com

class-map type urlfilter match-any trusted-domain-class
 match server-domain urlf-glob trusted-domain-param

parameter-map type urlf-glob untrusted-domain-param
 pattern www.example3.com
 pattern www.example4.com

class-map type urlfilter match-any untrusted-domain-class
 match server-domain urlf-glob untrusted-domain-param
```

Related Commands

Command	Description
class-map type urlfilter	Creates a class map to be used for matching packets to which a URL filtering policy applies.
match url-keyword urlf-glob	Specifies the match criteria for a local URL keyword filter.
parameter-map type urlf-glob	Specifies the per-policy parameters for local URL filtering of trusted domains, untrusted domains, and URL keywords.

match server-response any

To configure the match criterion for a SmartFilter (N2H2) or Websense URL filtering class map, use the **match server-response any** command in class-map configuration mode. To remove the match criterion, use the **no** form of this command.

match server-response any

no match server-response any

Syntax Description

This command has no arguments or keywords.

Command Default

No match criterion is configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **match server-response any** command to specify that any response from the SmartFilter or Websense server results in a match. Use this command after you have created a class map with the **class-map type urlfilter n2h2** or the **class-map type urlfilter websense** command:

Examples

The following example shows the configuration for a SmartFilter class:

```
class-map type urlfilter n2h2 match-any smartfilter-class
 match server-response any
```

The following example shows the configuration for a Websense class:

```
class-map type urlfilter websense match-any websense-class
 match server-response any
```

Related Commands

Command	Description
class-map type urlfilter	Creates a class map to which a URL filtering policy applies.

match service

To specify a match criterion for any supported Instant Messenger (IM) protocol, use the **match service** command in class-map configuration mode. To remove the match criterion from the configuration file, use the **no** form of this command.

match service {**any** | **text-chat**}

no match service {**any** | **text-chat**}

Syntax Description

any	Matches any type of service within the given IM protocol with the exception of text chat messages.
text-chat	Matches packets for text chat messages.

Command Default

None

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.4(20)T	Support for I Seek You (ICQ) and Windows Messenger IM Protocols was added.

Usage Guidelines

Use the **match service** command to configure the Cisco IOS Firewall to create a match criterion on the basis of text chat messages or for any available service within a given IM protocol.

Before you can use the **match service** command, you must issue the **class-map type inspect** command and specify one of the following IM protocols: AOL, ICQ, MSN Messenger, Yahoo Messenger, and Windows Messenger.

Examples

The following example shows how to configure an AOL IM policy that permits text chat and blocks any MSN IM service:

```
class-map type inspect aol match-any l7cmap-service-text-chat
 match service text-chat
!
class-map type inspect msnmsgr match-any l7cmap-service-any
 match service any

! Allow text-chat, reset if any other service, alarm for both
policy-map type inspect im l7pmap
class type inspect aol l7cmap-service-text-chat
allow
log
!
```

```
class type inspect msnmsgr l7cmap-service-any
reset
log
```

Related Commands

Command	Description
class-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect type class map.

match text-chat

To use text chat messages as the match criterion, use the **match text-chat** command in class-map configuration mode. To remove the match criterion from the configuration file, use the **no** form of this command.

match text-chat [*regular-expression*]

no match text-chat [*regular-expression*]

Syntax Description

regular-expression	(Optional) The regular expression used to identify specific eDonkey text chat messages. For example, entering ".exe" as the regular expression would classify the eDonkey text chat messages containing the string ".exe" as matches for the traffic policy. To specify that all eDonkey text chat messages be identified by the traffic class, use an asterisk (*) as the regular expression.

Command Default

None

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Use the **match text-chat** command to configure the Cisco IOS firewall to block text chat messages between clients using the eDonkey peer-to-peer (P2P) application.

Note This command is available only for the eDonkey P2P protocol.

Examples

The following example shows how to configure all text chat messages to be classified into the "my-edonkey-exe" class map:

```
class-map type inspect edonkey match-any my-edonkey-exe
 match text-chat
```

Related Commands

Command	Description
class-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect type class map.

match url

To specify the URL to be associated with the URL profile that configures the SDP registrar to run HTTPS, use the **match url** command in tti-registrar configuration mode. To remove this configuration, use the **no** form of this command.

match url *url*

no match url *url*

Syntax Description

url	Specifies the URL to be associated with the URL profile.

Command Default

No URL is associated with the URL profile.

Command Modes

Tti-registrar configuration mode (tti-registrar)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **match url** command is required in the SDP registrar configuration, which is used to deploy Apple iPhones on a corporate network.

Examples

The following example configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network from global configuration mode:

```
Router(config)# crypto provisioning registrar
Router(tti-registrar)# url-profile start START
Router(tti-registrar)# url-profile intro INTRO
Router(tti-registrar)# match url /sdp/intro
Router(tti-registrar)# match authentication trustpoint apple-tp
Router(tti-registrar)# match certificate cat 10
Router(tti-registrar)# mime-type application/x-apple-aspen-config
Router(tti-registrar)# template location flash:intro.mobileconfig
Router(tti-registrar)# template variable p iphone-vpn
```

Related Commands

Command	Description
crypto provisioning registrar	Configures a device to become a registrar for the SDP exchange and enters tti-registrar configuration mode.
url-profile	Specifies a URL profile that configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network.
match authentication trustpoint	Enters the trustpoint name that should be used to authenticate the peer's certificate.

Command	Description
match certificate	Enters the name of the certificate map used to authorize the peer's certificate.
mime-type	Specifies the MIME type that the SDP registrar should use to respond to a request received through the URL profile.
template location	Specifies the location of the template that the SDP Registrar should use while responding to a request received through the URL profile.
template variable p	Specifies the value that goes into the OU field of the subject name in the certificate to be issued.

match url category

To configure the match criteria for a Trend-Micro URL filtering class map on the basis of the specified URL category, use the **match url category** command in class-map configuration mode. To remove the URL category match criteria from a URL filtering class map, use the **no** form of this command.

match url category *category-name*

no match url category *category-name*

Syntax Description

category-name	Name of the URL category.

Command Default

No match criteria are configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **match url category** command specifies the name of the URL category to be used as the match criteria against which packets are checked to determine whether they belong to the class specified by the class map. Before you can use the **match url category** command, you must first use the **class-map type urlfilter** command to specify the name of the class whose match criteria you want to establish.

To display a list of supported URL categories, use the **match url category ?** command in class map configuration mode.

Examples

The following example specifies a class map for Trend Micro filtering called drop-category and configures the URL categories Gambling and Personals-Dating as match criteria:

```
class-map type urlfilter trend match-any drop-category
 match url category Gambling
 match url category Personals-Dating
```

Related Commands

Command	Description
class-map type urlfilter	Creates a class map to be used for matching packets to which a URL filtering policy applies.
match url reputation	Specifies a match criterion for a URL filtering class map on the basis of URL reputation.

match url-keyword urlf-glob

To configure the match criteria for a local URL filtering class map on the basis of the URL keyword, use the **match url-keyword urlf-glob** command in class-map configuration mode. To remove the keyword match criteria from a URL filtering class map, use the **no** form of this command.

match url-keyword urlf-glob *parameter-map-name*

no match url-keyword urlf-glob *parameter-map-name*

Syntax Description

parameter-map-name	Name of the parameter map.

Command Default

No match criteria are configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **match url-keyword urlf-glob** command specifies URL keyword matches for local URL filtering. Typically, you use this command to specify the URL keywords for which you want to block access. You must configure the **urlf-glob** keyword with the **parameter-map type urlf-glob** command and create the local filtering class with the **class-map type urlfilter** command before using this command, otherwise you will receive an error message.

Examples

The following example shows the use of:

- The **parameter-map type urlf-glob** command to configure the the keyword matching patterns.
- The **class-map type urlfilter** command to create the local URL filtering class keyword class.
- The **match url-keyword urlf-glob** command to specify the matching criteria for the class.

```
parameter-map type urlf-glob keyword-param
 pattern example
 pattern www.example1
 pattern example3

class-map type urlfilter match-any keyword-class
 match url-keyword urlf-glob keyword-param
```

Related Commands

Command	Description
class-map type urlfilter	Creates a class map to be used for matching packets to which a URL filtering policy applies.
match server-domain urlf-glob	Specifies the match criteria for a local domain name filter.
parameter-map type urlf-glob	Specifies the per-policy parameters for local URL filtering of trusted domains, untrusted domains, and URL keywords.

match url reputation

To configure the match criteria for a Trend-Micro URL filtering class map on the basis of the specified URL reputation, use the **match url reputation** command in class-map configuration mode. To remove the URL reputation match criteria from a URL filtering class map, use the **no** form of this command.

match url reputation *reputation-name*

no match url reputation *reputation-name*

Syntax Description

reputation-name	Name of the URL reputation.

Command Default

No match criteria are configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **match url reputation** command specifies the name of the URL reputation to be used as a match criterion against which packets are checked to determine whether they belong to the class specified by the class map. Before you can use the **match url reputation** command, you must first use the **class-map type urlfilter** command to specify the name of the class whose match criteria you want to establish.

To display a list of supported URL reputations, use the **match url reputation ?** command in class map configuration mode.

Examples

The following example specifies a class map for Trend Micro filtering called drop-reputation and configures the URL reputations ADWARE and PHISHING as match criteria:

```
class-map type urlfilter trend match-any drop-reputation
 match url reputation ADWARE
 match url reputation PHISHING
```

Related Commands

Command	Description
class-map type urlfilter	Creates a class map to be used for matching packets to which a URL filtering policy applies.
match url category	Specifies a match criterion for a URL filtering class map on the basis of URL category.

match user-group

To configure the match criterion for a class map on the basis of the specified user group, use the **match user-group** command in class-map configuration mode. To remove user-group based match criterion from a class map, use the **no** form of this command.

match user-group *group-name*

no match user-group *group-name*

Syntax Description

group-name	Name of the user-group used as a matching criterion.

Command Default

No match criterion is configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

To use the **match user-group** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish.

Examples

The following example specifies a class map called ftp and configures the user-group as a match criterion:

```
Router(config)# class-map type inspect match-all auth_proxy_ins_cm
Router(config-cmap)# description
!
Inspect Type Class-map for auth_proxy_ug
!
Router(config-cmap)# match protocol telnet
Router(config-cmap)# match user-group auth_proxy_ug
Router(config-cmap)# exit
Router(config)# class-map type inspect match-all eng_group_ins_cm
Router(config-cmap)# description
!
Inspect Type Class-map for eng_group_ug
!
Router(config-cmap)# match protocol telnet
Router(config-cmap)# match user-group eng_group_ug
Router(config-cmap)# exit
Router(config)# class-map type inspect match-all manager_group_ins_cm
Router(config-cmap)# description
!
Inspect Type Class-map for manager_group_ug
!
Router(config-cmap)# match protocol ftp
Router(config-cmap)# match user-group manager_group_ug
```

```
Router(config-cmap)# end
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
user-group	Defines the user-group associated with the identity policy.

max-destination

To configure the maximum number of destinations that a firewall can track, use the **max-destination** command in profile configuration mode. To disable the configuration, use the **no** form of this command.

max-destination *number*

no max-destination *number*

Syntax Description

number	Maximum destination value. Valid values are from 1 to 4294967295.

Command Default

The maximum number of destinations that a firewall can track is not configured.

Command Modes

Profile configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Usage Guidelines

You must configure the **parameter-map type inspect-zone** command before you can configure the **max-destination** command.

The firewall creates an entry for each destination to track the rate of TCP synchronization (SYN) flood packets arriving from a zone to a destination address. The number of entries that a firewall creates should be limited, so that these entries do not consume a lot of memory during a denial-of-service (DoS) attack. The **max-destination** command configures the maximum number of destinations that a firewall can track. When the maximum limit is reached, the SYN packets to a destination are dropped.

Examples

The following example shows how to set the maximum number of destinations that a firewall can track to 10000:

```
Router(config)# parameter-map type inspect-zone
Router(config-profile)# max-destination 10000
Router(config-profile)# end
```

Related Commands

Command	Description
parameter-map type inspect-zone	Configures a parameter map of type inspect zone and enters profile configuration mode.

max-header-length

To permit or deny HTTP traffic on the basis of the message header length, use the **max-header-length** command in appfw-policy-http configuration mode. To disable this inspection parameter, use the **no** form of this command.

max-header-length request *bytes* **response** *bytes* **action** {**reset** | **allow**} [**alarm**]

no max-header-length request *bytes* **response** *bytes* **action** {**reset** | **allow**} [**alarm**]

Syntax Description

request *bytes*	Maximum header length, in bytes, allowed in the request message. Number of bytes range: 0 to 65535.
response *bytes*	Maximum header length, in bytes, allowed in the response message. Number of bytes range: 0 to 65535.
action	Messages that exceed the maximum size are subject to the specified action (**reset** or **allow**).
reset	Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection.
allow	Forwards the packet through the firewall.
alarm	(Optional) Generates system logging (syslog) messages for the given action.

Defaults

If this command is not issued, all traffic is permitted.

Command Modes

appfw-policy-http configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

All message header lengths exceeding the configured maximum size will be subjected to the specified action (**reset** or **allow**).

Examples

The following example shows how to define the HTTP application firewall policy “mypolicy.” This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule “firewall,” which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
```

```
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

max-incomplete

To define the number of existing half-open sessions that will cause the Cisco IOS firewall to start and stop deleting half-open sessions, use the **max-incomplete** command in parameter-map type inspect configuration mode. To disable this function, use the **no** form of this command.

max-incomplete {**low** *number-of-connections* | **high** *number-of-connections*}

no max-incomplete {**low** *number-of-connections* | **high** *number-of-connections*}

Syntax Description

low *number-of-connections*	Minimum number of half-open sessions that will cause the Cisco IOS firewall to stop deleting half-open sessions. The default is unlimited.
high *number-of-connections*	Maximum number of half-sessions after which the Cisco IOS firewall will start deleting half-open sessions. The default is unlimited.

Command Default

The maximum number is unlimited and no half-open sessions are deleted.

Command Modes

Parameter-map type inspect configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

When you are configuring an inspect type parameter map, you can enter the **max-incomplete** subcommand after you enter the **parameter-map type inspect** command.

Enter the **max-incomplete** command twice. The first command specifies a high number at which the system will start deleting half-open sessions. The second command specifies a low number at which the system will stop deleting half-open sessions.

For more detailed information about creating a parameter map, see the **parameter-map type inspect** command.

Examples

The following example shows how to specify that the Cisco IOS firewall will stop deleting half-open sessions when there is a minimum of 800 half-open sessions and a maximum of 10000 half-open sessions:

```
parameter-map type inspect internet-policy
 max-incomplete high 10000
 max-incomplete low unlimited 800
```

Related Commands

Command	Description
ip inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ip inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

max-logins

To limit the number of simultaneous logins for users in a specific server group, use the **max-logins** command in global configuration mode. To remove the number of connections that were set, use the **no** form of this command.

max-logins *number-of-users*

no max-logins *number-of-users*

Syntax Description

number-of-users	Number of logins. The value ranges from 1 through 10.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

The **crypto isakmp client configuration group** command must be configured before this command can be configured.

This command makes it possible to mimic the functionality provided by some RADIUS servers for limiting the number of simultaneous logins for users in that group.

The **max-users** and **max-logins** keywords can be enabled together or individually to control the usage of resources by any groups or individuals.

Examples

The following example shows that the maximum number of logins for users in server group “cisco” has been set to 8:

```
Router (config)# crypto isakmp client configuration group cisco
Router (config)# max-logins 8
```

The following shows the RADIUS attribute-value (AV) pairs for the maximum users and maximum logins parameters:

```
ipsec:max-users=1000
ipsec:max-logins=1
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.
max-users	Limits the number of connections to a specific server group.

max-request

To specify the maximum number of outstanding requests that can exist at any given time, use the **max-request** command in URL parameter-map configuration mode. To disable this feature, use the **no** form of this command.

max-request *number-of-requests*

no max-request *number-of-requests*

Syntax Description

number-of-requests	Maximum number of pending requests that can be queued to the urlfiltering server.

Command Default

None

Command Modes

URL parameter-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

When you are creating or modifying a URL parameter map, you can enter the **max-request** subcommand after you enter the **parameter-map type urlfilter** command. For more detailed information about creating a parameter map, see the **parameter-map type urlfilter** command.

Examples

The following example specifies that there can be a maximum of 80 outstanding requests at a given time:

```
parameter-map type urlfilter u1
 max-request 80
```

Related Commands

Command	Description
parameter-map type urlfilter	Creates or modifies a parameter map for URL filtering parameters.

max-resp-pak

To specify the maximum number of HTTP responses that the Cisco IOS firewall can keep in its packet buffer, use the **max-resp-pak** command in URL parameter-map configuration mode. To disable this feature, use the **no** form of this command.

max-resp-pak *number-of-responses*

no max-resp-pak *number-of-responses*

Syntax Description

number-of-responses	Maximum number of HTTP responses that the firewall can keep in its packet buffer before it starts dropping responses.

Command Default

None

Command Modes

URL parameter-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

When you are creating or modifying a URL parameter map, you can enter the **max-resp-pak** subcommand after you enter the **parameter-map type urlfilter** command. For more detailed information about creating a parameter map, see the **parameter-map type urlfilter** command.

Examples

The following example specifies that there can be a maximum of 200 HTTP responses in the packet buffer:

```
parameter-map type urlfilter eng-filter-profile
 max-resp-pak 200
```

Related Commands

Command	Description
parameter-map type urlfilter	Creates or modifies a parameter map for URL filtering parameters.

max-retry-attempts

To set the maximum number of retries before Single SignOn (SSO) authentication fails, use the **max-retry-attempts** command in webvpn sso server configuration mode. To remove the number of retries that were set, use the **no** form of this command.

max-retry-attempts *number-of-retries*

no max-retry-attempts *number-of-retries*

Syntax Description

number-of-retries	Number of retries. Value = 1 through 5. Default = 3.

Command Default

A maximum number of retries is not set. If this command is not configured, the default is 3 retries.

Command Modes

Webvpn sso server configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

This command is useful for networks that are congested and tend to have losses. Corporate networks are generally not affected by congestion or losses.

Examples

The following example shows that the maximum number of retries is 3:

```
webvpn context context1
 sso-server test-sso-server
  max-retry-attempts 3
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

max-uri-length

To permit or deny HTTP traffic on the basis of the uniform resource identifier (URI) length in the request message, use the **max-uri-length** command in appfw-policy-http configuration mode. To disable this inspection parameter, use the **no** form of this command.

max-uri-length *bytes* **action** {**reset** | **allow**} [**alarm**]

no max-uri-length *bytes* **action** {**reset** | **allow**} [**alarm**]

Syntax Description

bytes	Number of bytes ranging from 0 to 65535.
action	Messages that exceed the maximum URI length are subject to the specified action (**reset** or **allow**).
reset	Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection.
allow	Forwards the packet through the firewall.
alarm	(Optional) Generates system logging (syslog) messages for the given action.

Defaults

If this command is not issued, all traffic is permitted.

Command Modes

appfw-policy-http configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

All URI lengths exceeding the configured value will be subjected to the specified action (**reset** or **allow**).

Examples

The following example shows how to define the HTTP application firewall policy “mypolicy.” This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule “firewall,” which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
```

```
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

max-users

To limit the number of connections to a specific server group, use the **max-users** command in global configuration mode. To remove the number of connections that were set, use the **no** form of this command.

max-users *number-of-users*

no max-users *number-of-users*

Syntax Description

number-of-users	Number of users. The value ranges from 1 through 5000.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

The **crypto isakmp client configuration group** command must be configured before this command can be configured.

This command makes it possible to mimic the functionality provided by some RADIUS servers for limiting the number of connections to a specific server group.

The **max-users** and **max-logins** keywords can be enabled together or individually to control the usage of resources by any groups or individuals.

Examples

The following example shows that the maximum number of connections to server group “cisco” has been set to 1200:

```
Router (config)# crypto isakmp client configuration group cisco
Router (config)# max-users 1200
```

The following shows the RADIUS attribute-value (AV) pairs for the maximum users and maximum logins parameters:

```
ipsec:max-users=1000
ipsec:max-logins=1
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.
max-logins	Limits the number of simultaneous logins for users in a specific server group.

max-users (WebVPN)

To limit the number of connections to an SSL VPN that will be permitted, use the **max-users** command in webvpn context configuration mode. To remove the connection limit from the SSL VPN context configuration, use the **no** form of this command.

max-users *number*

no max-users

Syntax Description

number	Maximum number of SSL VPN user connections. A number from 1 to 1000 can be entered for this argument.

Command Default

The following is the default if this command is not configured or if the **no** form is entered:

number : 1000

Command Modes

Webvpn context configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following example configures a limit of 500 user connections that will be accepted by the SSL VPN:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# max-users 500
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

mime-type

To specify the Multipurpose Internet Mail Extensions (MIME) type that the SDP registrar should use to respond to a request received through the URL profile, use the **mime-type** command in tti-registrar configuration mode. To remove this configuration, use the **no** form of this command.

mime-type *mime-type*

no mime-type *mime-type*

Syntax Description

mime-type	Specifies the MIME type.

Command Default

No MIME type is configured for the SDP registrar.

Command Modes

Tti-registrar configuration mode (tti-registrar)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **mime-type** command is required in the SDP registrar configuration, which is used to deploy Apple iPhones on a corporate network.

Examples

The following example configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network from global configuration mode:

```
Router(config)# crypto provisioning registrar
Router(tti-registrar)# url-profile start START
Router(tti-registrar)# url-profile intro INTRO
Router(tti-registrar)# match url /sdp/intro
Router(tti-registrar)# match authentication trustpoint apple-tp
Router(tti-registrar)# match certificate cat 10
Router(tti-registrar)# mime-type application/x-apple-aspen-config
Router(tti-registrar)# template location flash:intro.mobileconfig
Router(tti-registrar)# template variable p iphone-vpn
```

Related Commands

Command	Description
crypto provisioning registrar	Configures a device to become a registrar for the SDP exchange and enters tti-registrar configuration mode.
url-profile	Specifies a URL profile that configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network.
match authentication trustpoint	Enters the trustpoint name that should be used to authenticate the peer's certificate.

Command	Description
match certificate	Enters the name of the certificate map used to authorize the peer's certificate.
match url	Specifies the URL to be associated with the URL profile.
template location	Specifies the location of the template that the SDP Registrar should use while responding to a request received through the URL profile.
template variable p	Specifies the value that goes into the OU field of the subject name in the certificate to be issued.

mls acl tcam default-result

To set the default action during the ACL TCAM update, use the **mls acl tcam default-result** command in global configuration mode. To return to the default settings, use the **no** form of this command.

mls acl tcam default-result {**permit** | **deny** | **bridge**}

no mls acl tcam default-result

Syntax Description

permit	Permits all traffic.
deny	Denies all traffic.
bridge	Bridges all Layer 3 traffic up to the rendezvous point.

Defaults

deny

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

In the transition time between when an existing ACL is removed and a new ACL is applied, a default **deny** is programmed in the hardware. Once the new ACL has been applied completely in the hardware, the default **deny** is removed.

Use the **mls acl tcam default-result permit** command to permit all traffic in the hardware or bridge all traffic to the software during the transition time.

Examples

This example shows how to permit all traffic to pass during the ACL TCAM update:

```
Router(config)# mls acl tcam default-result permit
```

This example shows how to deny all traffic during the ACL TCAM update:

```
Router(config)# mls acl tcam default-result deny
```

This example shows how to bridge all Layer 3 traffic up to the rendezvous point during the ACL TCAM update:

```
Router(config)# mls acl tcam default-result bridge
```

mls acl tcam override dynamic dhcp-snooping

To allow web-based authentication (webauth) and IP Source Guard (IPSG) to function together on the same interface, use the **mls acl tcam override dynamic dhcp-snooping** command in global configuration mode. To disable this compatibility function, use the **no** form of this command.

mls acl tcam override dynamic dhcp-snooping

no mls acl tcam override dynamic dhcp-snooping

Syntax Description

This command has no arguments or keywords.

Command Default

This function is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXI2	This command was introduced.

Usage Guidelines

On the Catalyst 6500 series switch, when both webauth and IPSG are configured on the same access port and DHCP snooping is enabled on the access VLAN, the webauth downloadable ACLs (DACLs) can interfere with the DHCP snooping functionality. To prevent this interference, enter the **mls acl tcam override dynamic dhcp-snooping** command in global configuration mode. This command causes DHCP snooping entries to be replicated in the DACLs.

Examples

This example shows how to configure compatibility between webauth and IPSG:

```
Router(config)# mls acl tcam override dynamic dhcp-snooping
```

Related Commands

Command	Description
ip admission	Configures web-based authentication on the interface.
ip dhcp snooping	Enables DHCP snooping.
ip verify source	Enables IP Source Guard on the port.

mls acl tcam share-global

To enable sharing of the global default ACLs, use the **mls acl tcam share-global** command in global configuration mode. To turn off sharing of the global defaults, use the **no** form of this command.

mls acl tcam share-global

no mls acl tcam share-global

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you power cycle one of the DFCs, we recommend that you reset all the DFCs across the ACLs of the different DFCs.

Examples

This example shows how to enable sharing of the global default ACLs:

```
Router(config)# mls acl tcam share-global
```

mls acl vacl apply-self

To enable VACL lookups on software-switched and router-generated packets on the Catalyst 6500 Supervisor Engine 2, use the **mls acl vacl apply-self** command in global configuration mode. To disable VACL lookups for software packets, use the **no** form of this command.

mls acl vacl apply-self

no mls acl vacl apply-self

Syntax Description

This command has no keywords or arguments.

Defaults

VACL lookup on the egress VLAN for software packets are not enabled on switches with Supervisor Engine 2.

Command Modes

Global configuration

Command History

Release	Modification
12.2SXF15	Support for this command was introduced on the Supervisor Engine 2.

Usage Guidelines

On the Supervisor Engine 2 based switches running Cisco IOS Release 12.2(18)SXF15 or a later release, you can enable VACL lookups on software-switched and router generated packets for the VLAN filter configured on the egress VLAN by entering the **mls acl vacl apply-self** command.

On both the Supervisor Engine 720 and Supervisor Engine 32, software-switched packets and router-generated packets are always subjected to VACL lookups on the egress VLAN.

Examples

This example shows how to enable VACL lookups on software-switched and router-generated packets:

```
Router(config)# mls acl vacl apply-self
Router(config)#
```

mls aclmerge algorithm

To select the type of ACL merge method to use, use the **mls aclmerge algorithm** command in global configuration mode.

mls aclmerge algorithm {**bdd** | **odm**}

Syntax Description

bdd	Specifies the binary decision diagram (BDD)-based algorithm.
odm	Specifies the order dependent merge (ODM)-based algorithm.

Defaults

bdd

Command Modes

Global configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

The BDD-based ACL merge uses Boolean functions to condense entries into a single merged list of Ternary Content Addressable Memory (TCAM) entries that can be programmed into the TCAM.

You cannot disable the ODM-based ACL merge on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

The ODM-based ACL merge uses an order-dependent merge algorithm to process entries that can be programmed into the TCAM.

Note The ODM-based ACL merge supports both security ACLs and ACLs that are used for QoS filtering.

If you change the algorithm method, the change is not retroactive. For example, ACLs that have had the merge applied are not affected. The merge change applies to future merges only.

Use the **show fm summary** command to see the status of the current merge method.

Examples

This example shows how to select the BDD-based ACL to process ACLs:

```
Router(config)# mls aclmerge algorithm bdd
The algorithm chosen will take effect for new ACLs which are being applied, not
for already applied ACLs.
Router(config)
```

This example shows how to select the ODM-based ACL merge to process ACLs:

```
Router(config)# mls aclmerge algorithm odm
The algorithm chosen will take effect for new ACLs which are being applied, not
for already applied ACLs.
```

Related Commands

Command	Description
show fm summary	Displays a summary of feature manager information.

mls ip acl port expand

To enable ACL-specific features for Layer 4, use the **mls ip acl port expand** command in global configuration mode. To disable the ACL-specific Layer 4 features, use the **no** form of this command.

mls ip acl port expand

no mls ip acl port expand

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to enable the expansion of ACL logical operations on Layer 4 ports:

```
Router(config)# mls ip acl port expand
```

mls ip inspect

To permit traffic through any ACLs that would deny the traffic through other interfaces from the global configuration command mode, use the **mls ip inspect** command. Use the **no** form of this command to return to the default settings.

mls ip inspect *acl-name*

no mls ip inspect *acl-name*

Syntax Description

acl-name	ACL name.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Releae 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

On a Cisco 7600 series router, when interfaces are configured to deny traffic, the CBAC permits traffic to flow bidirectionally only through the interface that is configured with the **ip inspect** command.

Examples

This example shows how to permit the traffic through a specific ACL (named den-ftp-c):

```
Router(config)# mls ip inspect deny-ftp-c
Router(config)#
```

Related Commands

Command	Description
ip inspect	Applies a set of inspection rules to an interface.

mls rate-limit all

To enable and set the rate limiters common to unicast and multicast packets in the global configuration command mode, use the **mls rate-limit all** command. Use the **no** form of this command to disable the rate limiters.

mls rate-limit all {**mtu-failure** | **ttl-failure**} *pps* [*packets-in-burst*]

no mls rate-limit all {**mtu-failure** | **ttl-failure**}

Syntax Description

all	Specifies rate limiting for unicast and multicast packets.
mtu-failure	Enables and sets the rate limiters for MTU-failed packets.
ttl-failure	Enables and sets the rate limiters for TTL-failed packets.
pps	Packets per second; valid values are from 10 to 1000000 packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Defaults

The Layer 2 rate limiters are off by default. If you enable and set the rate limiters, the default *packets-in-burst* is **10**.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Rate limiters can rate-limit packets that are punted from the data path in the hardware up to the data path in the software. Rate limiters protect the control path in the software from congestion by dropping the traffic that exceeds the configured rate.

Note For Cisco 7600 series routers configured with a PFC3A, enabling the Layer 2 rate limiters has a negative impact on the multicast traffic. This negative impact does not apply to Cisco 7600 series routers configured with a PFC3BXL.

Examples

This example shows how to set the TTL-failure limiter for unicast and multicast packets:

```
Router(config)# mls rate-limit all ttl-failure 15
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit layer2

To enable and rate limit the control packets in Layer 2, use the **mls rate-limit layer2** command in global configuration mode. To disable the rate limiter in the hardware, use the **no** form of this command.

mls rate-limit layer2 {**ip-admission | l2pt | pdu | port-security| unknown**} *pps* [*packets-in-burst*]

no mls rate-limit layer2 [**l2pt | pdu | port-security | unknown**]

Syntax Description

ip-admission *pps*	Specifies the rate limit for IP admission on Layer 2 ports; valid values are from 10 to 1000000 packets per second.
l2pt *pps*	Specifies the rate limit for control packets in Layer 2 with a protocol-tunneling multicast-MAC address in Layer 2; valid values are from 10 to 1000000 packets per second.
pdu *pps*	Specifies the rate limit for Bridge Protocol Data Unit (BPDU), Cisco Discovery Protocol (CDP), Protocol Data Unit (PDU), and VLAN Trunk Protocol (VTP) PDU Layer 2 control packets; valid values are from 10 to 1000000 packets per second.
port-security *pps*	Specifies the rate limit for port security traffic; valid values are from 10 to 1000000 packets per second.
unknown	Specifies the rate limit for unknown unicast flooding on Layer 2 ports; valid values are from 10 to 1000000 packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Defaults

The Layer 2 rate limiters are off by default. If you enable and set the rate limiters, the default *packets-in-burst* value is 10 and *pps* value has no default setting.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(17a)SX	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2(18)SXF5	This **port-security** keyword was added.
12.2(33)SXH	The **ip-admission** keyword was added.

Usage Guidelines

MLS provides high-performance hardware-based Layer 3 switching at Layer 2.

This command is not supported on Catalyst 6500 series switches and Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The **unknown** keyword is only available on PFC3C line cards. When PFC3C and PFC3B linecards are powered on in the same chassis the chassis will downgrade to the PFC3B linecard and the **unknown** keyword will be unavailable.

You cannot configure the Layer 2 rate limiters if the global switching mode is set to truncated mode.

The following restrictions are pertinent to the use of the **port-security** *pps* keywords and argument:

- The PFC2 does not support the port-security rate limiter.
- The truncated switching mode does not support the port-security rate limiter.
- The lower the value, the more the CPU is protected.

Rate limiters control packets as follows:

- The frames are classified as Layer 2 control frames by the destination MAC address. The destination MAC address used are as follows:
  - 0180.C200.0000 for IEEE BPDU
  - 0100.0CCC.CCCC for CDP
  - 0100.0CCC.CCCD for Per VLAN Spanning Tree (PVST)/Shared Spanning Tree Protocol (SSTP) BPDU
- The software allocates an Local Target Logic (LTL) index for the frames.
- The LTL index is submitted to the forwarding engine for aggregate rate limiting of all the associated frames.

The Layer 2 control packets are as follows:

- General Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP)
- BPDUs
- CDP/Dynamic Trunking Protocol (DTP)/Port Aggregation Protocol (PAgP)/UniDirectional Link Detection Protocol (UDLD)/Link Aggregation Control Protocol (LACP) /VTP PDUs
- PVST/SSTP PDUs

If the rate of the traffic exceeds the configured rate limit, the excess packets are dropped at the hardware.

The **pdu** and **l2pt** rate limiters use specific hardware rate-limiter numbers only, such as 9 through 12. Enter the **show mls rate-limit usage** command to display the available rate-limiter numbers. The available numbers are displayed as “Free” in the output field. If all four of those rate limiters are in use by other features, a system message is displayed telling you to turn off a feature to rate limit the control packets in Layer 2.

When a MAC move occurs and a packet is seen on two ports, the packet is redirected to the software. If one of those ports has the violation mode set to restrict or protect, the packet is dropped in software. You can use the port-security rate limiter to throttle the number of such packets redirected to software. This helps in protecting the software from high traffic rates.

Examples

This example shows how to enable and set the rate limiters for the protocol-tunneling packets in Layer 2:

```
Router(config)# mls rate-limit layer2 l2pt 3000
```

This example shows how to configure the **port-security** rate limiter:

```
Router(config)# mls rate-limit layer2 port-security 500
```

This example shows how to configure the **ip-admission** rate limiter:

```
Router(config)# mls rate-limit layer2 ip-admission 560
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit unicast l3-features

To enable and set the Layer 3 security rate limiters for the unicast packets in the global configuration command mode, use the **mls rate-limit unicast l3-features** command. Use the **no** form of this command to disable the rate limiters.

mls rate-limit unicast l3-features *pps* [*packets-in-burst*]

no mls rate-limit unicast l3-features *pps* [*packets-in-burst*]

Syntax Description

pps	Packets per second; see the "Usage Guidelines" section for valid values.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Defaults

The defaults are as follows:

- Enabled at **2000** *pps* and *packets-in-burst* is set to **1**.
- If the *packets-in-burst* is not set, **10** is programmed for unicast cases.

Command Modes

Global configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

Examples

This example shows how to set the Layer 3 security rate limiters for the unicast packets:

```
Router(config)# mls rate-limit unicast l3-features 5000
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit multicast ipv4

To enable and set the rate limiters for the IPv4 multicast packets in the global configuration command mode, use the **mls rate-limit multicast ipv4** command. Use the **no** form of this command to disable the rate limiters.

mls rate-limit multicast ipv4 {**connected** | **fib-miss** | **igmp** | **ip-option** | **partial** | **non-rpf**} *pps* [*packets-in-burst*]

no mls rate-limit multicast ipv4 {**connected** | **fib-miss** | **igmp** | **ip-option** | **partial** | **non-rpf**}

Syntax Description

connected	Enables and sets the rate limiters for multicast packets from directly connected sources.
fib-miss	Enables and sets the rate limiters for the FIB-missed multicast packets.
igmp	Enables and sets the rate limiters for the IGMP packets.
ip-option	Enables and sets the rate limiters for the multicast packets with IP options.
partial	Enables and sets the rate limiters for the multicast packets during a partial SC state.
non-rpf	Enables and sets the rate limiters for the multicast packets failing the RPF check.
pps	Packets per second; valid values are from 10 to 1000000 packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Defaults

The defaults are as follows:

- If the *packets-in-burst* is not set, a default of **100** is programmed for multicast cases.
- **fib-miss**—Enabled at **100000** *pps* and *packet-in-burst* is set to **100**.
- **ip-option**—Disabled.
- **partial**—Enabled at **100000** *pps* and *packet-in-burst* is set to **100**.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17b)SXA	This command was changed to support the **igmp** and **ip-option** keywords.
12.2(18)SXD	This command was changed to include the **ipv4** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

You cannot configure the IPv4 rate limiters if the global switching mode is set to truncated mode.

The rate limiters can rate limit the packets that are punted from the data path in the hardware up to the data path in the software. The rate limiters protect the control path in the software from congestion and drop the traffic that exceeds the configured rate.

The **ip-option** keyword is supported in PFC3BXL or PFC3B mode only.

Examples

This example shows how to set the rate limiters for the multicast packets failing the RPF check:

```
Router(config)# mls rate-limit multicast ipv4 non-rpf 100
Router(config)#
```

This example shows how to set the rate limiters for the multicast packets during a partial SC state:

```
Router(config)# mls rate-limit multicast ipv4 partial 250
Router(config)#
```

This example shows how to set the rate limiters for the FIB-missed multicast packets:

```
Router(config)# mls rate-limit multicast ipv4 fib-miss 15
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit multicast ipv6

To configure the IPv6 multicast rate limiters, use the **mls rate-limit multicast ipv6** command in global configuration mode. To disable the rate limiters, use the **no** form of this command.

mls rate-limit multicast ipv6 {**connected** *pps* [*packets-in-burst*] | *rate-limiter-name* {**share** {**auto** | *target-rate-limiter*}}

no mls rate-limit multicast ipv6 {**connected** | *rate-limiter-name*}

Syntax Description

connected *pps*	Enables and sets the rate limiters for the IPv6 multicast packets from a directly connected source; valid values are from 10 to 1000000 packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.
rate-limiter-name	Rate-limiter name; valid values are **default-drop**, **route-cntl**, **secondary-drop**, **sg**, **starg-bridge**, and **starg-m-bridge**. See the "Usage Guidelines" section for additional information.
share	Specifies the sharing policy for IPv6 rate limiters; see the "Usage Guidelines" section for additional information.
auto	Decides the sharing policy automatically.
target-rate-limiter	Rate-limiter name that was the first rate-limiter name programmed in the hardware for the group; valid values are **default-drop**, **route-cntl**, **secondary-drop**, **sg**, **starg-bridge**, and **starg-m-bridge**. See the "Usage Guidelines" section for additional information.

Command Default

If the *burst* is not set, a default of **100** is programmed for multicast cases.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXD	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The *rate-limiter-name* argument must be a rate limiter that is not currently programmed.

The *target-rate-limiter* argument must be a rate limiter that is programmed in the hardware and must be the first rate limiter programmed for its group.

Table 43 lists the IPv6 rate limiters and the class of traffic that each rate limiter serves.

Table 43 IPv6 Rate Limiters

Rate-Limiter ID	Traffic Classes to be Rate Limited
Connected	Directly connected source traffic
Default-drop	* (*, G/m)SSM * (*, G/m)SSM non-rpf
Route-control	* (*, FF02::X/128)
Secondary-drop	* (*, G/128) SPT threshold is infinity
SG	* (S, G) RP-RPF post-switchover * (*, FFx2/16)
Starg-bridge	* (*, G/128) SM * SM non-rpf traffic when (*, G) exists
Starg-M-bridge	* (*, G/m) SM * (*, FF/8) * SM non-rpf traffic when (*, G) does not exist

You can configure rate limiters for IPv6 multicast traffic using one of the following methods:

- Direct association of the rate limiters for a traffic class—Select a rate and associate the rate with a rate limiter. This example shows how to pick a rate of 1000 pps and 20 packets per burst and associate the rate with the **default-drop** rate limiter:

  ```
  Router(config)# mls rate-limit multicast ipv6 default-drop 1000 20
  ```

- Static sharing of a rate limiter with another preconfigured rate limiter—When there are not enough adjacency-based rate limiters available, you can share a rate limiter with an already configured rate limiter (target rate limiter). This example shows how to share the **route-cntl** rate limiter with the **default-drop** target rate limiter:

  ```
  Router(config)# mls rate-limit multicast ipv6 route-cntl share default-drop
  ```

  If the target rate limiter is not configured, a message displays that the target rate limiter must be configured for it to be shared with other rate limiters.

- Dynamic sharing of rate limiters—If you are not sure about which rate limiter to share with, use the **share auto** keywords to enable dynamic sharing. When you enable dynamic sharing, the system picks a preconfigured rate limiter and shares the given rate limiter with the preconfigured rate limiter. This example shows how to choose dynamic sharing for the **route-cntrl** rate limiter:

  ```
  Router(config)# mls rate-limit multicast ipv6 route-cntl share auto
  ```

Examples

This example shows how to set the rate limiters for the IPv6 multicast packets from a directly connected source:

```
Router(config)# mls rate-limit multicast ipv6 connected 1500 20
Router(config)#
```

This example shows how to configure a direct association of the rate limiters for a traffic class:

```
Router(config)# mls rate-limit multicast ipv6 default-drop 1000 20
Router(config)#
```

This example shows how to configure the static sharing of a rate limiter with another preconfigured rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share default-drop
Router(config)#
```

This example shows how to enable dynamic sharing for the **route-cntrl** rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share auto
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit unicast acl

To enable and set the ACL-bridged rate limiters in global configuration command mode, use the **mls rate-limit unicast acl** command. Use the **no** form of this command to disable the rate limiters.

mls rate-limit unicast acl {**input** | **output** | **vacl-log**} *pps* [*packets-in-burst*]

Syntax Description

input	Specifies the rate limiters for the input ACL-bridged unicast packets.
output	Specifies the rate limiters for the output ACL-bridged unicast packets.
vacl-log	Specifies the rate limiters for the VACL log cases.
pps	Packets per second; see the "Usage Guidelines" section for valid values.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Defaults

The defaults are as follows:

- **input**—Disabled.
- **output**—Disabled.
- **vacl-log**—Enabled at **2000** *pps* and *packets-in-burst* is set to **1**.
- If the *packets-in-burst* is not set, **10** is programmed for unicast cases.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	The **mls rate-limit unicast** command was reformatted.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

The **input** and **output** keywords are not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The rate limiters can rate limit the packets that are punted from the data path in the hardware up to the data path in the software. The rate limiters protect the control path in the software from congestion and drop the traffic that exceeds the configured rate.

When setting the *pps*, valid values are as follows:

- ACL input and output cases—10 to 1000000 *pps*
- VACL log cases—10 to 5000 *pps*

You cannot change the **vacl-log** *packets-in-burst* keyword and argument; it is set to **1** by default.

Some cases (or scenarios) share the same hardware register. These cases are divided into the following two groups:

- Group1:
  - Egress ACL-bridged packets
  - Ingress ACL-bridged packets
- Group 2:
  - RPF failure
  - ICMP unreachable for ACL drop
  - ICMP unreachable for no-route
  - IP errors

All the components of each group use or share the same hardware register. For example, ACL-bridged ingress and egress packets use register A. ICMP-unreachable, no-route, and RPF failure use register B.

In most cases, when you change a component of a group, all the components in the group are overwritten to use the same hardware register as the first component changed. A warning message is printed out each time that an overwriting operation occurs, but only if you enable the service internal mode. The overwriting operation does not occur in these situations:

- The *pps* value is set to **0** (zero) for a particular case.
- When the ingress or egress ACL-bridged packet cases are disabled, overwriting does not occur until the cases are enabled again. If either case is disabled, the other is not affected as long as the remaining case is enabled. For example, if you program the ingress ACL-bridged packets with a 100-pps rate, and then you configure the egress ACL-bridged packets with a 200-pps rate, the ingress ACL-bridged packet value is overwritten to 200 pps and both the ingress and the egress ACL-bridged packets have a 200-pps rate.

Examples

This example shows how to set the input ACL-bridged packet limiter for unicast packets:

```
Router(config)# mls rate-limit unicast acl input 100
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit unicast cef

To enable and set the Cisco Express Forwarding rate limiters in global configuration command mode, use the **mls rate-limit unicast cef** command. Use the **no** form of this command to disable the rate limiters.

mls rate-limit unicast cef {**receive** | **glean**} *pps* [*packets-in-burst*]

Syntax Description

receive	Enables and sets the rate limiters for receive packets.
glean	Enables and sets the rate limiters for ARP-resolution packets.
pps	Packets per second; valid values are from 10 to 1000000 packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Defaults

The defaults are as follows:

- **receive**—Disabled.
- **glean**—Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(17a)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB. The default for **glean** was changed to disabled.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

If you enable the CEF rate limiters, the following behaviors occur (if the behavior that is listed is unacceptable, disable the CEF rate limiters):

- If a packet hits a glean/receive adjacency, the packet may be dropped instead of being sent to the software if there is an output ACL on the input VLAN and the matched entry result is deny.
- If the matched ACL entry result is bridge, the packet is subject to egress ACL bridge rate limiting (if turned ON) instead of glean/receive rate limiting.
- The glean/receive adjacency rate limiting is applied only if the output ACL lookup result is permit or there is no output ACLs on the input VLAN.

Examples

This example shows how to set the CEF-glean limiter for the unicast packets:

```
Router(config)# mls rate-limit unicast cef glean 5000
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit unicast ip

To enable and set the rate limiters for the unicast packets in global configuration command mode, use the **mls rate-limit unicast ip** command. Use the **no** form of this command to disable the rate limiters.

mls rate-limit unicast ip {**errors** | **features** | **options** | **rpf-failure**} *pps* [*packets-in-burst*]

mls rate-limit unicast ip icmp {**redirect** | **unreachable acl-drop** *pps* | **no-route** *pps*} [*packets-in-burst*]

no mls rate-limit unicast ip {**errors** | **features** | **icmp** {**redirect** | **unreachable** {**acl-drop** | **no-route**}} | **options** | **rpf-failure**} *pps* [*packets-in-burst*]

Syntax Description

errors	Specifies rate limiting for unicast packets with IP checksum and length errors.
features	Specifies rate limiting for unicast packets with software-security features in Layer 3 (for example, authorization proxy, IPsec, and inspection).
options	Specifies rate limiting for unicast IPv4 packets with options.
rpf-failure	Specifies rate limiting for unicast packets with RPF failures.
pps	Packets per second; see the "Usage Guidelines" section for valid values.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.
icmp redirect	Specifies rate limiting for unicast packets requiring ICMP redirect.
icmp unreachable acl-drop *pps*	Enables and sets the rate limiters for the ICMP unreachables for the ACL-dropped packets.
icmp unreachable no-route *pps*	Enables and sets the rate limiters for the ICMP unreachables for the FIB-miss packets.

Defaults

The defaults are as follows:

- If the *packets-in-burst* is not set, a default of **10** is programmed as the burst for unicast cases.
- **errors**—Enabled at **500** *pps* and *packets-in-burst* set to **10**.
- **rpf-failure**—Enabled at **500** *pps* and *packets-in-burst* set to **10**.
- **icmp unreachable acl-drop**—Enabled at **500** *pps* and *packets-in-burst* set to **10**.
- **icmp unreachable no-route**—Enabled at **500** *pps* and *packets-in-burst* set to **10**.
- **icmp redirect**—Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	The **mls rate-limit unicast** command added the **ip** keyword to the following: • **options** • **icmp** • **rpf-failure** • **errors** • **features** These keywords were changed as follows: • The **features** keyword replaced the **l3-features** keyword. • The **mls rate-limit unicast icmp redirect** command replaced the **mls rate-limit unicast icmp-redirect** command. • The **mls rate-limit unicast icmp unreachable** command replaced the **mls rate-limit unicast icmp-unreachable** command.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

To provide OAL support for denied packets, enter the **mls rate-limit unicast ip icmp unreachable acl-drop 0** command.

OAL and VACL capture are incompatible. Do not configure both features on the switch. With OAL configured, use SPAN to capture traffic.

The rate limiters can rate limit the packets that are punted from the data path in the hardware up to the data path in the software. The rate limiters protect the control path in the software from congestion and drop the traffic that exceeds the configured rate.

Note When you configure an ICMP rate limiter, and an ICMP redirect occurs, exiting data traffic is dropped while the remaining traffic on the same interface is forwarded.

When setting the *pps*, the valid values are **0** and from 10 to 1000000. Setting the *pps* to **0** globally disables the redirection of the packets to the route processor. The **0** value is supported for these rate limiters:

- ICMP unreachable ACL-drop
- ICMP unreachable no-route
- ICMP redirect
- IP rpf failure

Some cases (or scenarios) share the same hardware register. These cases are divided into the following two groups:

- Group1:
  - Egress ACL-bridged packets
  - Ingress ACL-bridged packets
- Group 2:
  - RPF failure
  - ICMP unreachable for ACL drop
  - ICMP unreachable for no-route
  - IP errors

All the components of each group use or share the same hardware register. For example, ACL-bridged ingress and egress packets use register A. ICMP-unreachable, no-route, and RPF failure use register B.

In most cases, when you change a component of a group, all the components in the group are overwritten to use the same hardware register as the first component changed. A warning message is printed out each time that an overwriting operation occurs, but only if you enable the service internal mode. The overwriting operation does not occur in these situations:

- The *pps* value is set to **0** (zero) for a particular case.
- When the ingress or egress ACL-bridged packet cases are disabled, overwriting does not occur until the cases are enabled again. If either case is disabled, the other is not affected as long as the remaining case is enabled. For example, if you program the ingress ACL-bridged packets with a 100-pps rate, and then you configure the egress ACL-bridged packets with a 200-pps rate, the ingress ACL-bridged packet value is overwritten to 200 pps and both the ingress and the egress ACL-bridged packets have a 200-pps rate.

Examples

This example shows how to set the ICMP-redirect limiter for unicast packets:

```
Router(config)# mls rate-limit unicast ip icmp redirect 250
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit unicast vacl-log

To enable and set the VACL-log case rate limiters in the global configuration command mode, use the **mls rate-limit unicast vacl-log** command. Use the **no** form of this command to disable the rate limiters.

mls rate-limit unicast vacl-log *pps* [*packets-in-burst*]

Syntax Description

pps	Packets per second; see the "Usage Guidelines" section for valid values.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Defaults

The defaults are as follows:

- Enabled at **2000** *pps* and *packets-in-burst* is set to **1**.
- If the *packets-in-burst* is not set, **10** is programmed for unicast cases.

Command Modes

Global configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

The rate limiters can rate limit the packets that are punted from the data path in the hardware up to the data path in the software. The rate limiters protect the control path in the software from congestion and drop the traffic that exceeds the configured rate.

When setting the *pps*, valid values are as follows:

- ACL input and output cases—10 to 1000000 *pps*
- VACL log cases—10 to 5000 *pps*

Setting the *pps* to **0** globally disables the redirection of the packets to the route processor.

You cannot change the **vacl-log** *packets-in-burst* keyword and argument; it is set to **1** by default.

Some cases (or scenarios) share the same hardware register. These cases are divided into the following two groups:

- Group1:
  - Egress ACL-bridged packets
  - Ingress ACL-bridged packets

- Group 2:
  - RPF failure
  - ICMP unreachable for ACL drop
  - ICMP unreachable for no-route
  - IP errors

All the components of each group use or share the same hardware register. For example, ACL-bridged ingress and egress packets use register A. ICMP-unreachable, no-route, and RPF failure use register B.

In most cases, when you change a component of a group, all the components in the group are overwritten to use the same hardware register as the first component changed. A warning message is printed out each time that an overwriting operation occurs, but only if you enable the service internal mode. The overwriting operation does not occur in these situations:

- The *pps* value is set to **0** (zero) for a particular case.
- When the ingress or egress ACL-bridged packet cases are disabled, overwriting does not occur until the cases are enabled again. If either case is disabled, the other is not affected as long as the remaining case is enabled. For example, if you program the ingress ACL-bridged packets with a 100-pps rate, and then you configure the egress ACL-bridged packets with a 200-pps rate, the ingress ACL-bridged packet value is overwritten to 200 pps and both the ingress and the egress ACL-bridged packets have a 200-pps rate.

Examples

This example shows how to set the VACL-log case packet limiter for unicast packets:

```
Router(config)# mls rate-limit unicast vacl-log 100
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mode (IPSec)

To change the mode for a transform set, use the **mode** command in crypto transform configuration mode. To reset the mode to the default value of tunnel mode, use the **no** form of this command.

mode [**tunnel** | **transport**]

no mode

Syntax Description

tunnel | **transport**	(Optional) Specifies the mode for a transform set: either tunnel or transport mode. If neither **tunnel** nor **transport** is specified, the default (tunnel mode) is assigned.

Defaults

Tunnel mode

Command Modes

Crypto transform configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to change the mode specified for the transform. This setting is only used when the traffic to be protected has the same IP addresses as the IPSec peers (this traffic can be encapsulated either in tunnel or transport mode). This setting is ignored for all other traffic (all other traffic is encapsulated in tunnel mode).

If the traffic to be protected has the same IP address as the IP Security peers and transport mode is specified, during negotiation the router will request transport mode but will accept either transport or tunnel mode. If tunnel mode is specified, the router will request tunnel mode and will accept only tunnel mode.

After you define a transform set, you are put into the crypto transform configuration mode. While in this mode you can change the mode to either tunnel or transport. This change applies only to the transform set just defined.

If you do not change the mode when you first define the transform set, but later decide you want to change the mode for the transform set, you must re-enter the transform set (specifying the transform name and all its transforms) and then change the mode.

If you use this command to change the mode, the change will only affect the negotiation of subsequent IPSec security associations via crypto map entries which specify this transform set. (If you want the new settings to take effect sooner, you can clear all or part of the security association database. See the **clear crypto sa** command for more details.

Tunnel Mode

With tunnel mode, the entire original IP packet is protected (encrypted, authenticated, or both) and is encapsulated by the IPSec headers and trailers (an Encapsulation Security Protocol header and trailer, an Authentication Header, or both). Then a new IP header is prefixed to the packet, specifying the IPSec endpoints as the source and destination.

Tunnel mode can be used with any IP traffic. Tunnel mode must be used if IPSec is protecting traffic from hosts behind the IPSec peers. For example, tunnel mode is used with Virtual Private Networks (VPNs) where hosts on one protected network send packets to hosts on a different protected network via a pair of IPSec peers. With VPNs, the IPSec peers "tunnel" the protected traffic between the peers while the hosts on their protected networks are the session endpoints.

Transport Mode

With transport mode, only the payload (data) of the original IP packet is protected (encrypted, authenticated, or both). The payload is encapsulated by the IPSec headers and trailers (an ESP header and trailer, an AH header, or both). The original IP headers remain intact and are not protected by IPSec.

Use transport mode only when the IP traffic to be protected has IPSec peers as both the source and destination. For example, you could use transport mode to protect router management traffic. Specifying transport mode allows the router to negotiate with the remote peer whether to use transport or tunnel mode.

Examples

The following example defines a transform set and changes the mode to transport mode. The mode value only applies to IP traffic with the source and destination addresses at the local and remote IPSec peers.

```
crypto ipsec transform-set newer esp-des esp-sha-hmac
 mode transport
 exit
```

Related Commands

Command	Description
crypto ipsec transform-set	Defines a transform set—an acceptable combination of security protocols and algorithms.

mode ra

To place the public key infrastructure (PKI) server into Registration Authority (RA) certificate server mode, use the **mode ra** command in certificate server configuration mode. To remove the PKI server from RA certificate mode, use the **no** form of this command.

mode ra [**transparent**]

no mode ra [**transparent**]

Syntax Description

transparent	The **transparent** keyword allows the CA server in RA mode to interoperate with more than one type of CA server.

Defaults

The PKI server is not placed into RA certificate server mode.

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
15.1(2)T	This command was modified. In Cisco IOS Release 15.1(2)T, the **transparent** keyword was introduced that allows the IOS CA server in RA mode to interoperate with more than one type of CA server.

Usage Guidelines

When this command is configured, ensure that the **crypto pki trustpoint** command has also been configured and that the enrollment URL is pointed to a Cisco IOS issuing certification authority (CA). If the **mode ra** command is not configured and the certificate server is enabled for the first time, a self-signed CA certificate will be generated and the certificate server will operate as a root CA.

The Cisco IOS certificate server can act as an RA for a Cisco IOS CA or another third party CA. The **transparent** keyword is used if a third-party CA is used.

When the **transparent** keyword is used, the original PKCS#10 enrollment message is not re-signed and is forwarded unchanged. This enrollment message makes the IOS RA certificate server work with CA servers like the Microsoft CA server.

Examples

The following configuration example shows that a RA mode certificate server named "myra" has been configured:

```
Router (config)# crypto pki trustpoint myra
Router (ca-trustpoint)# enrollment url http://10.3.0.6
Router (ca-trustpoint)# subject-name cn=myra, ou=ioscs RA, o=cisco, c=us
Router (ca-trustpoint)# exit

Router (config)# crypto pki server myra
Router (cs-server)# mode ra
Router (cs-server)# no shutdown
```

Related Commands:

Command	Description
crypto pki server	Enables a Cisco IOS certificate server.
crypto pki trustpoint	Declares the trustpoint that your router should use.
enrollment	Specifies the enrollment parameters of a CA.
show crypto pki server	Displays the current state and configuration of the certificate server.

mode secure

To enable the secure mode in the Lightweight Directory Access Protocol (LDAP) server, use the **mode secure** command in LDAP server configuration mode. To disable the secure mode in LDAP server, use the **no** form of this command.

mode secure [**no-negotiation**]

no mode secure [**no-negotiation**]

Syntax Description

no-negotiation	(Optional) Specifies the Transport Layer Security (TLS) specific parameter.

Command Default

The secure mode is disabled.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

Use the **mode secure** command to establish a TLS connection with the LDAP server. This command will help to secure all the transactions.

Examples

The following example shows how to configure the secure mode on the LDAP server:

```
Router(config)# ldap server server1
Router(config-ldap-server)# mode secure no-negotiation
```

Related Commands

Command	Description
ldap server	Defines an LDAP server and enters LDAP server configuration mode.

mode sub-cs

To place the public key infrastructure (PKI) server into sub-certificate server mode, use the **mode sub-cs** command in certificate server mode. To remove the PKI server from sub-certificate mode, use the **no** form of this command.

mode sub-cs

no mode sub-cs

Syntax Description

This command has no arguments or keywords.

Defaults

The PKI server is not placed into sub-certificate server mode.

Command Modes

Certificate server

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

When this command is configured, ensure that the **crypto pki trustpoint** command has also been configured and that the enrollment URL is pointed to a Cisco IOS root certification authority (CA). If the **mode sub-cs** command is not configured and the certificate server is enabled for the first time, a self-signed CA certification will be generated and the certificate server will operate as a root CA.

Note The **no mode sub-cs** command will have no effect if the server has been configured already. For example, if you want to make the subordinate CA a root CA, you must delete the server and re-create it.

Examples

The following configuration example shows that a subordinate certificate server named “sub” has been configured:

```
Router (config)# crypto pki trustpoint sub
Router (ca-trustpoint)# enrollment url http://10.3.0.6
Router (ca-trustpoint)# exit

Router (config)# crypto pki server sub
Router (cs-server)# issuer-name CN=sub CA, O=Cisco, C=us
Router (cs-server)# mode sub-cs
Router (cs-server)# no shutdown
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server.
crypto pki trustpoint	Declares the trustpoint that your router should use.

Command	Description
enrollment	Specifies the enrollment parameters of a CA.
issuer-name	Specifies the DN as the CA issuer name for the certificate server.
show crypto pki server	Displays the current state and configuration of the certificate server.

monitor event-trace dmvpn

To monitor and control Dynamic Multipoint VPN (DMVPN) traces, use the **monitor event-trace dmvpn** command in privileged EXEC or global configuration mode.

Privileged EXEC

monitor event-trace dmvpn {**dump** [**merged**] **pretty** | {**nhrp** {**error** | **event** | **exception**} | **tunnel**} {**clear** | **continuous** [**cancel**] | **disable** | **enable** | **one-shot**} | **tunnel**}}

Global Configuration

monitor event-trace dmvpn {**dump-file** *url* | {**nhrp** {**error** | **event** | **exception**} | **tunnel**} {**disable** | **dump-file** *url* | **enable** | **size** | **stacktrace** *value*}}

no monitor event-trace dmvpn {**dump-file** *url* | {**nhrp** {**error** | **event** | **exception**} | **tunnel**} {**disable** | **dump-file** *url* | **enable** | **size** | **stacktrace** *value*}}

Syntax Description

dump	Displays all event traces.
merged	(Optional) Displays entries in all the event traces sorted by time.
pretty	Displays the event traces in ASCII format.
nhrp	Monitors Next Hop Resolution Protocol (NHRP) traces.
error	Monitors NHRP error traces.
event	Monitors NHRP event traces.
exception	Monitors NHRP exception errors.
tunnel	Monitors all tunnel events.
clear	Clears the trace.
continuous	Displays the latest event trace entries continuously.
cancel	(Optional) Cancels continuous display of the latest trace entries.
disable	Disables NHRP or tunnel tracing.
enable	Enables NHRP or tunnel tracing.
one-shot	Clears the trace, sets the running configuration, and then disables the configuration at the wrap point.
tunnel	Monitors all tunnel events.
dump-file *url*	Sets the name of the dump file.
stacktrace *value*	Specifies the trace buffer stack to be cleared first. The stack range is from 1 to 16.

Command Default

DMVPN event tracing is disabled.

Command Modes

Privileged EXEC (#)
Global configuration (config)

Command History

Release	Modification
15.1(4)M	This command was introduced.

Usage Guidelines

You can use the **monitor event-trace dmvpn** command to configure the DMVPN Event Tracing feature. The DMVPN Event Tracing feature provides a trace facility for troubleshooting Cisco IOS DMVPN. This feature enables you to monitor DMVPN events, errors, and exceptions. During runtime, the event trace mechanism logs trace information in a buffer space. A display mechanism extracts and decodes the debug data.

Note You can configure the DMVPN Event Tracing feature in privileged EXEC mode or global configuration mode based on the desired parameters.

Examples

The following example shows how to configure a router to monitor and control NHRP event traces in privileged EXEC mode:

```
Router# monitor event-trace dmvpn nhrp event enable
```

The following example shows how to configure a router to monitor and control NHRP exception traces in privileged EXEC mode:

```
Router# monitor event-trace dmvpn nhrp exception enable
```

The following example shows how to configure a router to monitor and control NHRP error traces in privileged EXEC mode:

```
Router# monitor event-trace dmvpn nhrp error enable
```

The following example shows how to configure a router to monitor and control NHRP event traces in global configuration mode:

```
Router# enable
Router(config)# monitor event-trace dmvpn nhrp event enable
```

The following example shows how to configure a router to monitor and control NHRP exception traces in global configuration mode:

```
Router# enable
Router(config)# monitor event-trace dmvpn nhrp exception enable
```

The following example shows how to configure a router to monitor and control NHRP error traces in global configuration mode:

```
Router# enable
Router(config)# monitor event-trace dmvpn nhrp error enable
```

Related Commands

Command	Description
show monitor event-trace dmvpn	Displays DMVPN trace information.

name

To configure the redundancy group with a name, use the **name** command in redundancy application group configuration mode**.** To remove the name of a redundancy group, use the **no** form of this command.

name *group-name*

no name *group-name*

SyntaxDescription

group-name	Name of the redundancy group.

Command Default

The redundancy group is not configured with a name.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following example shows how to configure the redundancy group name as group1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# name group1
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
group	Enters redundancy application group configuration mode.
shutdown	Shuts down a group manually.

name (view)

To change the name of a lawful intercept view, use the **name** command in view configuration mode. To return to the default lawful intercept view name, which is "li-view," use the **no** form of this command.

name *new-name*

no name *new-name*

Syntax Description

new-name	Lawful intercept view name.

Defaults

A lawful intercept view is called "li-view."

Command Modes

View configuration (config-view)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Only a system administrator or a level 15 privilege user can change the name of a lawful intercept view.

Examples

The following example shows how to configure a lawful intercept view and change the view name to "myliview":

```
!Initialize the LI-View.
Router(config-view)# li-view lipass user li_admin password li_adminpass
00:19:25:%PARSER-6-LI_VIEW_INIT:LI-View initialized.
Router(config-view)# name myliview
Router(config-view)# end
```

Related Commands

Command	Description
li-view	Initializes a lawful intercept view.
parser view	Creates or changes a CLI view and enters view configuration mode.

named-key

To specify which peer's RSA public key you will manually configure and enter public key configuration mode, use the **named-key** command in public key chain configuration mode. This command should be used only when the router has a single interface that processes IP Security (IPSec).

named-key *key-name* [**encryption** | **signature**]

Syntax Description

key-name	Specifies the name of the remote peer's RSA keys. This is always the fully qualified domain name of the remote peer; for example, router.example.com.
encryption	(Optional) Indicates that the RSA public key to be specified will be an encryption special-usage key.
signature	(Optional) Indicates that the RSA public key to be specified will be a signature special-usage key.

Defaults

If neither the **encryption** nor the **signature** keyword is used, general-purpose keys will be specified.

Command Modes

Public key chain configuration.

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command or the **addressed-key** command to specify which IPSec peer's RSA public key you will manually configure next.

Follow this command with the **key-string** command to specify the key.

If you use the **named-key** command, you also need to use the **address** public key configuration command to specify the IP address of the peer.

If the IPSec remote peer generated general purpose RSA keys, do not use the **encryption** or **signature** keyword.

If the IPSec remote peer generated special usage keys, you must manually specify both keys: perform this command and the **key-string** command twice and use the **encryption** and **signature** keywords in turn.

Examples

The following example manually specifies the RSA public keys of two IPSec peers. The peer at 10.5.5.1 uses general-purpose keys, and the other peer uses special-purpose keys.

```
crypto key pubkey-chain rsa
```

```
 named-key otherpeer.example.com
 address 10.5.5.1
 key-string
005C300D 06092A86 4886F70D 01010105
00034B00 30480241 00C5E23B 55D6AB22
04AEF1BA A54028A6 9ACC01C5 129D99E4
64CAB820 847EDAD9 DF0B4E4C 73A05DD2
BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
D58AD221 B583D7A4 71020301 0001
quit
exit
 addressed-key 10.1.1.2 encryption
 key-string
00302017 4A7D385B 1234EF29 335FC973
2DD50A37 C4F4B0FD 9DADE748 429618D5
18242BA3 2EDFBDD3 4296142A DDF7D3D8
08407685 2F2190A0 0B43F1BD 9A8A26DB
07953829 791FCDE9 A98420F0 6A82045B
90288A26 DBC64468 7789F76E EE21
quit
 exit
 addressed-key 10.1.1.2 signature
 key-string
0738BC7A 2BC3E9F0 679B00FE 098533AB
01030201 42DD06AF E228D24C 458AD228
58BB5DDD F4836401 2A2D7163 219F882E
64CE69D4 B583748A 241BED0F 6E7F2F16
0DE0986E DF02031F 4B0B0912 F68200C4
C625C389 0BFF3321 A2598935 C1B1
quit
 exit
 exit
```

Related Commands

Command	Description
address	Specifies the IP address of the remote RSA public key of the remote peer you will manually configure.
addressed-key	Specifies the RSA public key of the peer you will manually configure.
crypto key pubkey-chain rsa	Enters public key configuration mode (to allow you to manually specify the RSA public keys of other devices).
key-string (IKE)	Specifies the RSA public key of a remote peer.
show crypto key pubkey-chain rsa	Displays peer RSA public keys stored on your router.

nas

To add an access point or router to the list of devices that use the local authentication server, use the **nas** command in local RADIUS server configuration mode. To remove the identity of the network access server (NAS) that is configured on the local RADIUS server, use the **no** form of this command.

nas *ip-address* **key** *shared-key*

no nas *ip-address* **key** *shared-key*

Syntax Description

ip-address	IP address of the access point or router.
key	Specifies a key.
shared-key	Shared key that is used to authenticate communication between the local authentication server and the access points and routers that use this authenticator.

Defaults

No default behavior or values

Command Modes

Local RADIUS server configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Examples

The following command adds the access point having the IP address 192.168.12.17 to the list of devices that use the local authentication server, using the shared key named shared256.

```
Router(config-radsrv)# nas 192.168.12.17 key shared256
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
radius-server host	Specifies the remote RADIUS server host.

Command	Description
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

nasi authentication

To enable authentication, authorization, and accounting (AAA) authentication for NetWare Asynchronous Services Interface (NASI) clients connecting to a router, use the **nasi authentication** command in line configuration mode. To return to the default, as specified by the **aaa authentication nasi** command, use the **no** form of the command.

nasi authentication {**default** | *list-name*}

no nasi authentication {**default** | *list-name*}

Syntax Description

default	Uses the default list created with the **aaa authentication nasi** command.
list-name	Uses the list created with the **aaa authentication nasi** command.

Defaults

Uses the default set with the **aaa authentication nasi** command.

Command Modes

Line configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(15)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is a per-line command used with AAA authentication that specifies the name of a list of authentication methods to try at login. If no list is specified, the default list is used, even if it is not specified in the command line. (You create defaults and lists with the **aaa authentication nasi** command.) Entering the **no** form of this command has the same effect as entering the command with the **default** argument.

Caution If you use a *list-name* value that was not configured with the **aaa authentication nasi** command, you will disable login on this line.

Before issuing this command, create a list of authentication processes by using the **aaa authentication nasi** global configuration command.

Examples

The following example specifies that the default AAA authentication be used on line 4:

```
line 4
 nasi authentication default
```

The following example specifies that the AAA authentication list called *list1* be used on line 7:

```
line 7
 nasi authentication list1
```

Related Commands

Command	Description
aaa authentication nasi	Specifies AAA authentication for NASI clients connecting through the access server.
ipx nasi-server enable	Enables NASI clients to connect to asynchronous devices attached to a router.
show ipx nasi connections	Displays the status of NASI connections.
show ipx spx-protocol	Displays the status of the SPX protocol stack and related counters.

nat (IKEv2 profile)

To configure Network Address Translation (NAT) keepalive for Internet Key Exchange Version 2 (IKEv2), use the **nat** command in IKEv2 profile configuration mode. To delete NAT keepalive configuration, use the **no** form of this command.

nat keepalive *interval*

no nat keepalive

Syntax Description

keepalive *interval*	Specifies the NAT keepalive interval in seconds.

Command Default

NAT keepalive is disabled.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S.	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to configure NAT keepalive. NAT keepalive configuration specified in an IKEv2 profile overrides the global configuration. NAT keepalive prevents the NAT translation entries from deletion in the absence of any traffic when there is NAT between IKE peers.

Examples

The following example shows how to specify the NAT keepalive interval:

```
Router(config)# crypto ikev2 profile prf1
Router(config-ikev2-profile)# nat keepalive 500
```

Related Commands

Command	Description
crypto ikev2 nat	Defines NAT keepalive globally for all peers.
crypto ikev2 profile	Defines an IKEv2 profile.

nbns-list

To enter the webvpn NBNS list configuration mode to configure a NetBIOS Name Service (NBNS) server list for Common Internet File System (CIFS) name resolution, use the **nbns-list** command in webvpn context configuration mode. To remove the NBNS server list from the SSL VPN context configuration, use the **no** form of this command.

nbns-list *name*

no nbns-list *name*

Syntax Description

name	Name of the NBNS list. The name can be up to 64 characters in length. This argument is case sensitive.

Command Default

Webvpn NBNS list configuration mode is not entered, and a NBNS server list cannot be configured.

Command Modes

Webvpn context configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The NBNS server list is used to configure a list of Windows Internet Name Service (WINS) to resolve Microsoft file-directory shares. Entering the **nbns-list** command places the router in webvpn NBNS list configuration mode. You can specify up to three NetBIOS name servers. A single server is configured as the master browser if multiple servers are specified in the server list.

Note NBNS and CIFS resolution is supported only on Microsoft Windows 2000 or Linux Samba servers.

Examples

The following example configures an NBNS server list:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# nbns-list SERVER_LIST
Router(config-webvpn-nbnslist)# nbns-server 172.16.1.1 master
Router(config-webvpn-nbnslist)# nbns-server 172.16.2.2 timeout 10 retries 5
Router(config-webvpn-nbnslist)# nbns-server 172.16.3.3 timeout 10 retries 5
Router(config-webvpn-nbnslist)#
```

Related Commands

Command	Description
nbns-server	Adds a server to an NBNS server list.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

nbns-list (policy group)

To attach a NetBIOS name service (NBNS) server list to a policy group configuration, use the **nbns-list** command in webvpn group policy configuration mode. To remove the NBNS server list from the policy group configuration, use the **no** form of this command.

nbns-list *name*

no nbns-list

Syntax Description

name	Name of the NBNS server list that was configured in webvpn context configuration mode.

Command Default

An NBNS server list is not attached to a policy group configuration.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The configuration of this command applies to only clientless mode configuration.

Examples

The following example applies the NBNS server list to the policy group configuration:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# nbns-list SERVER_LIST
Router(config-webvpn-nbnslist)# nbns-server 172.16.1.1 master
Router(config-webvpn-nbnslist)# nbns-server 172.16.2.2 timeout 10 retries 5
Router(config-webvpn-nbnslist)# nbns-server 172.16.3.3 timeout 10 retries 5
Router(config-webvpn-nbnslist)# exit
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# nbns-list SERVER_LIST
Router(config-webvpn-group)#
```

Related Commands

Command	Description
nbns-list	Enters webvpn NBNS list configuration mode to configure a NBNS server list for CIFS name resolution.
nbns-server	Adds a server to an NBNS server list.
policy group	Enters webvpn group policy configuration mode to configure a group policy.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

nbns-server

To add a server to a NetBIOS name service (NBNS) server list, use the **nbns-server** command in webvpn NBNS list configuration mode. To remove the server entry from the NBNS server list, use the **no** form of this command.

nbns-server *ip-address* [**master**] [**timeout** *seconds*] [**retries** *number*]

no nbns-server *ip-address* [**master**] [**timeout** *seconds*] [**retries** *number*]

Syntax Description

ip-address	The IPv4 address of the NetBIOS server.
master	(Optional) Configures a single NetBIOS server as the master browser.
timeout *seconds*	(Optional) Configures the length of time, in seconds, that the networking device will wait for a query reply before sending a query to another NetBIOS server. A number from 1 through 30 can be configured for this argument.
retries *number*	(Optional) Number of times that the specified NetBIOS server will be queried. A number from 0 through 10 can be configured for this argument. Entering the number 0 configures the networking device not to resend a query.

Command Default

The following default values are used if this command is not configured or if the **no** form is entered:

timeout 2
retries 2

Command Modes

Webvpn NBNS list configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The server specified with the *ip-address* argument can be a primary domain controller (PDC) in a Microsoft network. A Windows Internet Naming Service (WINS) server cannot and should not be specified. When multiple NBNS servers are specified, a single server is configured as master browser.

Examples

The following example adds three servers to an NBNS server list:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# nbns-list SERVER_LIST
Router(config-webvpn-nbnslist)# nbns-server 172.16.1.1 master
Router(config-webvpn-nbnslist)# nbns-server 172.16.2.2 timeout 10 retries 5
Router(config-webvpn-nbnslist)# nbns-server 172.16.3.3 timeout 10 retries 5
```

Related Commands

Command	Description
nbns-list	Enters webvpn NBNS list configuration mode to configure a NBNS server list for CIFS name resolution.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

netmask

To specify the subnet mask to be used by the client for local connectivity, use the **netmask** command in ISAKMP group configuration mode or IKEv2 authorization policy configuration mode. To disable the mask, use the **no** form of this command.

netmask *mask*

no netmask *mask*

Syntax Description

mask	Subnet mask address.

Command Default

Default mask is used.

Command Modes

ISAKMP group configuration (config-isakmp-group)
IKEv2 authorization policy configuration (config-ikev2-author-policy)

Command History

Release	Modification
12.2(8)T	This command was introduced on the Easy VPN remote.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to specify the subnet mask for the IP address assigned to the client.

Examples

The following example shows that the subnet mask 255.255.255.255 is to be downloaded to the client:

```
crypto isakmp client configuration group group1
 netmask 255.255.255.255
```

Related Commands

Command	Description
crypto ikev2 authorization policy	Specifies an IKEv2 authorization policy group.
crypto isakmp client configuration group	Specifies the DNS domain to which a group belongs.

no crypto engine software ipsec

To disable hardware crypto engine failover to the software crypto engine, use the **no crypto engine software ipsec** command in global configuration mode. To reenable failover, use the **crypto engine software ipsec** form of this command.

no crypto engine software ipsec

crypto engine software ipsec

Syntax Description

This command has no arguments or keywords.

Defaults

Failover is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1E	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command for those situations in which the amount of IP Security (IPSec) traffic is more than can be handled (because of bandwidth) by the software routines on the CPU.

Examples

The following example shows that hardware crypto engine failover to the software crypto engine has been disabled:

```
no crypto engine software ipsec
```

The following example shows that hardware crypto engine failover has been reenabled:

```
crypto engine software ipsec
```

Related Commands

Command	Description
crypto engine accelerator	Enables the onboard hardware accelerator of the router for IPSec encryption.

no crypto xauth

To ignore extended authentication (Xauth) during an Internet Key Exchange (IKE) Phase 1 negotiation, use the **no crypto xauth** command in global configuration mode. To consider Xauth proposals, use the **crypto xauth** command.

no crypto xauth *interface*

crypto xauth *interface*

Syntax Description

interface	Interface whose IP address is the local endpoint to which the remote peer will send IKE requests.

Defaults

No default behaviors or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **no** version of this command was introduced to support Unity clients that do not require Xauth when using Internet Security Association and Key Management Protocol (ISAKMP) profiles.

Note This command does not support loopback interfaces.

Examples

The following example shows that Xauth proposals on Ethernet 1/1 are to be ignored:

```
no crypto xauth Ethernet1/1
```

no ip inspect

To turn off Context-based Access Control (CBAC) completely at a firewall, use the **no ip inspect** command in global configuration mode.

no ip inspect

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Turn off CBAC with the **no ip inspect** global configuration command.

Note The **no ip inspect** command removes all CBAC configuration entries and resets all CBAC global timeouts and thresholds to the defaults. All existing sessions are deleted and their associated access lists are removed.

Examples

The following example turns off CBAC at a firewall:

```
no ip inspect
```

no ip ips sdf builtin

To instruct the router not to load the built-in signatures if it cannot find the specified signature definition files (SDFs), use the **no ip ips sdf builtin** command in global configuration mode.

no ip ips sdf builtin

Syntax Description

This command has no arguments or keywords.

Defaults

If the router fails to load the SDF, the router will load the default, built-in signatures.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Caution If the **no ip ips sdf builtin** command is issued and the router running Intrusion Prevention System (IPS) fails to load the SDF, you will receive an error message stating that IPS is completely disabled.

Examples

The following example shows how to instruct the router not to refer to the default, built-in signature if the attack-drop.sdf file fails to load:

```
Router(config) no ip ips sdf builtin
```

Related Commands

Command	Description
copy ips-sdf	Loads or saves the SDF in the router.
ip ips sdf location	Specifies the location in which the router will load the SDF.

object-group (Catalyst 6500 series switches)

To define object groups that you can use to optimize your configuration, use the **object-group** global configuration mode command. To remove object groups from the configuration use the **no** form of this command .

object-group ip {{**address** *obj-grp-id*} | {**port** *obj-grp-id*}}

no object-group ip {{**address** *obj-grp-id*} | {**port** *obj-grp-id*}}

Syntax Description

ip	Specifies the IP object group.
address *obj-grp-id*	Specifies the IP address of the object group and allows you to define the object group name and enter IP-address object-group configuration mode. See the "Usage Guidelines" section for more information.
port *obj-grp-id*	Specifies the IP port of the object group and allows you to create or modify a PBACL protocol port object group. See the "Usage Guidelines" section for more information.

Command Default

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	Yes	Yes	Yes	Yes	No

Command History

Release	Modification
12.2(33)SXH	This command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

This command supports IPv4 and IPv6 addresses.

Objects such as hosts, protocols, or services can be grouped, and then you can issue a single command using the group name to apply to every item in the group.

When you define a group with the **object-group** command and then use any security appliance command, the command applies to every item in that group. This feature can significantly reduce your configuration size.

Once you define an object group, you must use the **object-group** keyword before the group name in all applicable security appliance commands as follows:

```
Router# show running-config object-group group-name
```

where group-name is the name of the group.

This example shows the use of an object group once it is defined:

```
Router(config)# access-list access_list_name permit tcp any object-group group-name
```

In addition, you can group access list command arguments:

Individual Argument	Object Group Replacement
protocol	**object-group** *protocol*
host and subnet	**object-group** *network*
service	**object-group** *service*
icmp-type	**object-group** *icmp-type*

You can group commands hierarchically; an object group can be a member of another object group.

To use object groups, you must do the following:

- Use the **object-group** keyword before the object group name in all commands as follows:

  ```
  Router(config)# access-list acl permit tcp object-group remotes object-group locals
  object-group eng-svc
  ```

  where **remotes** and **locals** are sample object group names.

- The object group must be nonempty.
- You cannot remove or empty an object group if it is being used in a command.

Use the **exit**, **quit**, or any valid config-mode commands such as **access-list** to close an object-group mode and exit the object-group main command.

The **show running-config object-group** command displays all defined object groups by their grp-id when the **show running-config object-group** *group-id* command is entered, and by their group type when you enter the **show running-config object-group** *group-type* command. When you enter the **show running-config object-group** command without an argument, all defined object groups are shown.

Use the **clear configure object-group** command to remove a group of previously defined **object-group** commands. Without an argument, the **clear configure object-group** command lets you to remove all defined object groups that are not being used in a command. Use of the *group-type* argument removes all defined object groups that are not being used in a command for that group type only.

You can use all other security appliance commands in an object-group mode, including the **show running-config** and **clear configure** commands

Commands within the object-group mode appear indented when displayed or saved by the **show running-config object-group**, **write**, or **config** commands.

Commands within the object-group mode have the same command privilege level as the main command.

When you use more than one object group in an **access-list** command, the elements of all object groups that are used in the command are linked, starting with the elements of the first group with the elements of the second group, then the elements of the first and second groups together with the elements of the third group, and so on.

The starting position of the description text is the character right immediately following the white space (a blank or a tab) following the **description** keyword.

When you enter the **object-group ip address** command, the prompt changes to Router(config-ipaddr-ogroup)# and allows you to create or modify a PBACL protocol port object group.

The following IP address object-group configuration commands are available:

- **A.B.C.D**—Specifies the network address of the object-group members.
- **end**—Exits from configuration mode.
- **exit**—Exits from IP object-group configuration mode.
- **host** *address* or **host** *name*—Specifies the host address or name of the object-group member.
- **no**—Negates or sets the default values of a command.

Use the **no** form of the command to delete the object group with the specified name.

When you enter the **object-group ip port** command, the prompt changes to Router(config-port-ogroup)# and allows you to define the object group name and enter port object-group configuration mode. The following port object-group configuration commands are available:

- **end**—Exits from configuration mode.
- **eq** *number*—Matches only packets on a given port number; valid values are from 0 to 65535.
- **exit**—Exits from the IP object-group configuration mode.
- **gt** *number*—Matches only packets on a given port number; valid values are from 0 to 65535.
- **lt** *number*—Matches only packets with a lower port number; valid values are from 0 to 65535.
- **neq** *number*—Matches only packets with a lower port number; valid values are from 0 to 65535.
- **no**—Negates or sets default values of a command.
- **range** *number number*—Matches only packets in the range of port numbers; valid values are from 0 to 65535.

Use the **no** form of the command to delete the object group with the specified name.

Examples

This example shows how to create an object group with three hosts and a network address:

```
Router(config)# object-group ip address myAG
Router(config-ipaddr-pgroup)# host 10.20.20.1
Router(config-ipaddr-pgroup)# host 10.20.20.5
Router(config-ipaddr-pgroup)# 10.30.0.0 255.255.0.0
```

This example shows how to create a port object group that matches protocol port 100 and any port greater than 200, except 300:

```
Router(config)# object-group ip port myPG
Router(config-port-pgroup)# eq 100
Router(config-port-pgroup)# gt 200
Router(config-port-pgroup)# neq 300
```

Related Commands

Command	Description
clear configure object-group	Removes all the object group commands from the configuration.
group-object	Adds network object groups.
network-object	Adds a network object to a network object group.
port-object	Adds a port object to a service object group.
show running-config object-group	Displays the current object groups.

object-group network

To define network object groups for use in object group-based ACLs (OGACLs) and enter network object-group configuration mode (config-network-group), use the **object-group network** command in global configuration mode. To remove network object groups from the configuration, use the **no** form of this command.

object-group network *object-group-name*

no object-group network *object-group-name*

Syntax Description

object-group-name	Specifies a name for a network type of object group. *object-group-name* is a sequence of 1 to 64 characters consisting of letters, digits, underscores (_), dashes (-), or periods (.). *object-group-name* must start with a letter.

Command Default

No network object groups are created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.
15.0(1)M	This command was modified. The **any** command was added as a command in network object-group configuration mode.

Usage Guidelines

A network object group is a group of any of the following objects: hostnames, host IP addresses, subnets, ranges of IP addresses, or existing network object groups. A network object group is an ordered list and can be used in an ACL or in other commands. You can use a single command using the group name to apply to every object in the group.

This command supports only IPv4 addresses.

Commands within the network object-group mode appear indented when displayed or saved by the **write memory** or **show running-config** commands.

Commands within the network object-group mode have the same command privilege level as the main command.

When you enter the **object-group network** command, the command mode enters network object-group configuration mode (config-network-group) and allows you to populate or modify a network OGACL. The following commands are available in this mode:

- **any**—Specifies any IP address for an object group. The effect is to to allow any IP address in the range of 0.0.0.0 to 255.255.255.255 to be used in an object group.

  This command supports only IPv4 addresses.

- **description** *description-text*—Description of the object or object group (you can use up to 200 characters).

- **group-object** *nested-object-group-name*—Existing network object group (child) to be included in the current object group (parent).

  The type of child object group must match that of the parent (for example, if you are creating a network object group, you must specify another network object group as the child).

  You can use duplicated objects in an object group if it is because of the inclusion of group objects. For example, if object 1 is in both group A and group B, you can define a group C that includes both A and B. However, you cannot include a group object that causes the group hierarchy to become circular (for example, you cannot include group A in group B and then also include group B in group A).

  You can use an unlimited number of nested object groups (however, a maximum of two levels is recommended).

- **host** {*host-address* | *host-name*}—Host object. If you specify a host address, you must use an IPv4 address.

- *network-address* {*/nn* | *network-mask*}—Specifies a subnet object for the object group.

  When the command is used in the network-address /nn format to create a subnet object, for example 209.165.201.0 /27, the 27 most significant bits are allocated for the network prefix number, and the remaining 5 bits are reserved for host addressing. If the same subnet object is created using the network-address network-mask format of the command, the command appears as 209.165.201.31 255.255.255.224. In this case, the subnet mask is 255.255.255.224. The default subnet mask is 255.255.255.255.

  Using a subnet mask of 0.0.0.0 includes any address in the range 0.0.0.0 to 255.255.255.255 in the subnet object—this gives the subnet object the same range as the range specified by the **any** command.

  The network-address command supports only IPv4 addresses.

- **range** *host-address1 host-address2*—Species the range of host IP addresses for an object group.

  If the range specified is 0.0.0.0 to 255.255.255.255 this specifies that any IP address can be used as a host IP address—this has the same effect as the **any** command, which specifies that any IP address can be used.

  If the same IP address is used for host-address1 and host-address2, the effect is the same as using the **host** command—the identical IP address specified becomes the single host IP address for the object group.

  This command supports only IPv4 addresses.

Use the **no** form of the command to delete the object group with the specified name. (You cannot delete an object group that is being used within an ACL or a CPL policy.)

Examples

The following example shows how to configure a network object group named my_network_object_group that contains two hosts and a subnet as objects.

```
Router> enable
Router# configure terminal
Router(config)# object-group network my_network_object_group
Router(config-network-group)# host 10.20.20.1
Router(config-network-group)# host 10.20.20.5
Router(config-network-group)# 10.30.0.0 255.255.0.0
```

The following example shows how to configure a network object group named sjc_ftp_servers that contains two hosts , a subnet, and an existing object group (child) named sjc_eng_ftp_servers as objects.

```
Router> enable
Router# configure terminal
Router(config)#object-group network sjc_ftp_servers
Router(config-network-group)# host sjc.eng.ftp
Router(config-network-group)# host 172.23.56.195
Router(config-network-group)# 209.165.200.225 255.255.255.224
Router(config-network-group)# group-object sjc_eng_ftp_servers
```

The following example creates an object group called printer_users and specifies any IP address for the object group:

```
Router> enable
Router# configure terminal
Router(config)# object-group network printer_users
Router(config-network-group)# description sw_engineers
Router(config-network-group)# any
```

The following example creates an object group called printer_users and specifies a range of host IP addresses from 209.165.202.129 to 255.255.255.255 for the object group:

```
Router> enable
Router# configure terminal
Router(config)# object-group network printer_users
Router(config-network-group)# description sw_engineers
Router(config-network-group)# range 209.165.202.129 255.255.255.255
```

Related Commands

Command	Description
deny	Sets conditions in a named IP access list or OGACL that will deny packets.
ip access-group	Applies an ACL or OGACL to an interface or a service policy map.
ip access-list	Defines an IP access list or OGACL by name or number.
object-group service	Defines service object groups for use in OGACLs.
permit	Sets conditions in a named IP access list or OGACL that will permit packets.
show ip access-list	Displays the contents of IP access lists or OGACLs.
show object-group	Displays information about object groups that are configured.

object-group service

To define service object groups for use in object group-based ACLs (OGACLs), use the **object-group service** command in global configuration mode. To remove service object groups from the configuration, use the **no** form of this command.

object-group service *object-group-name*

no object-group service *object-group-name*

Syntax Description

object-group-name	Specifies a service type of object group.

Command Default

No service object groups are created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

A service object group is a group of any of the following objects:

- Source and destination protocol ports (such as Telnet or SNMP)
- ICMP types (such as echo, echo-reply, or host-unreachable)
- Top-level protocols (such as TCP, UDP, or ESP)
- Existing service object groups

A service object group is an ordered list and can be used in an ACL or other commands. You can use a single command using the group name to apply to every object in the group.

This command supports only IPv4 addresses.

Commands within the service object-group mode appear indented when displayed or saved by the **write** or **config** commands.

Commands within the service object-group mode have the same command privilege level as the main command.

When you use more than one object group in an **access-list** command, the elements of all object groups that are used in the command are linked, starting with the elements of the first group with the elements of the second group, then the elements of the first and second groups together with the elements of the third group, and so on.

When you enter the **object-group service** command, the prompt changes to `Router(config-service-group)#` and allows you to populate or modify a service OGACL. The following commands are available in this mode:

- **description** *description-text*—Description of the object or object group (you can use up to 200 characters).

- *protocol*—(Required) Specifies an IP protocol number or name. You can use any one of the following values:
  - *number*—IP protocol number. The range is 0 to 255.
  - **ahp**—Authentication Header Protocol.
  - **eigrp**—Cisco EIGRP routing protocol.
  - **esp**—Encapsulation Security Payload.
  - **gre**—Cisco GRE tunneling.
  - **igmp**—Internet Gateway Message Protocol.
  - **ip**—Any Internet Protocol.
  - **ipinip**—IP in IP tunneling.
  - **nos**—KA9Q NOS compatible IP over IP tunneling.
  - **ospf**—OSPF routing protocol.
  - **pcp**—Payload Compression Protocol.
  - **pim**—Protocol Independent Multicast.
- **tcp | udp | tcp-udp** [**source** {{[**eq**] | **lt** | **gt**} *port1* | **range** *port1 port2*}] [{[**eq**] | **lt** | **gt**} *port1* | **range** *port1 port2*]—Transmission Control Protocol, User Datagram Protocol, or both.
  - **source**—Specifies a source port or ports. Specifying a source port or ports is optional, but when specifying them, the **source** keyword is required. Specifying a destination port or ports is optional. To specify destination ports, you specify an optional or required operator and a port value or values.
  - *operator port1* [*port2*]—Use the following operator keywords to specify a port value or a range of ports:

    eq—Single port value *port1*. When no *operator* is specified, the default is **eq**. However, this keyword is always present in the configuration file.

    The following keywords are required when specifying a range of ports.

    range—Range of ports between *port1* and *port2*, inclusive.

    l**t**—All port values that are less than *port1*.

    gt—All port values that are greater than *port1*.
  - *port1* [*port2*]—Decimal number or name of a TCP and/or UDP service. The value of the number ranges from 0 to 65535. If a name is specified, the name must be one of the supported TCP or UDP port name (or both). If a number is specified, translation to its corresponding name (if one exists) based on the protocol type will be made when showing the object configuration.

  Following are the supported services for TCP:

  0-65535—Port number.

  bgp—Border Gateway Protocol (179).

  chargen—Character generator (19).

  cmd—Remote commands (rcmd, 514).

  daytime—Daytime (13).

  discard—Discard (9).

  domain—Domain Name Service (53).

drip—Dynamic Routing Information Protocol (3949).

echo—Echo (7).

exec—Exec (rsh, 512).

finger—Finger (79).

ftp—File Transfer Protocol (21).

ftp-data—FTP data connections (20).

gopher—Gopher (70).

hostname—NIC hostname server (101).

ident—Ident Protocol (113).

irc—Internet Relay Chat (194).

klogin—Kerberos login (543).

kshell—Kerberos shell (544).

login—Login (rlogin, 513).

lpd—Printer service (515).

nntp—Network News Transport Protocol (119).

pim-auto-rp PIM Auto-RP (496).

pop2—Post Office Protocol v2 (109).

pop3—Post Office Protocol v3 (110).

smtp—Simple Mail Transport Protocol (25).

sunrpc—Sun Remote Procedure Call (111).

tacacs—TAC Access Control System (49).

talk—Talk (517).

telnet—Telnet (23).

time—Time (37).

uucp—Unix-to-Unix Copy Program (540).

whois—Nicname (43).

www—World Wide Web (HTTP, 80).

Following are the supported services for UDP:

0-65535—Port number.

biff—Biff (mail notification, comsat, 512).

bootpc—Bootstrap Protocol (BOOTP) client (68).

bootps—Bootstrap Protocol (BOOTP) server (67).

discard—Discard (9).

dnsix—DNSIX security protocol auditing (195).

domain—Domain Name Service (DNS, 53).

echo—Echo (7).

isakmp—Internet Security Association and Key Management Protocol (500).

mobile-ip—Mobile IP registration (434).

nameserver—IEN116 name service (obsolete, 42).

netbios-dgm—NetBios datagram service (138).

netbios-ns—NetBios name service (137).

netbios-ss—NetBios session service (139).

non500-isakmp Internet Security Association and Key Management Protocol (4500).

ntp—Network Time Protocol (123).

pim-auto-rp—PIM Auto-RP (496).

rip—Routing Information Protocol (router, in.routed, 520).

snmp—Simple Network Management Protocol (161).

snmptrap—SNMP Traps (162).

sunrpc—Sun Remote Procedure Call (111).

syslog—System Logger (514).

tacacs—TAC Access Control System (49).

talk—Talk (517).

tftp—Trivial File Transfer Protocol (69).

time—Time (37).

who—Who service (rwho, 513).

xdmcp—X Display Manager Control Protocol (177).

Following are the supported services for TCP and UDP:

0-**65535**—Port number.

discard—Discard (9).

domain—Domain Name Service (53).

echo—Echo (7).

pim-auto-rp—PIM Auto-RP (496).

sunrpc—Sun Remote Procedure Call (111).

syslog—Syslog (514).

tacacs—TAC Access Control System (49).

talk—Talk (517).

- **icmp** *icmp-type*—Decimal number or name of an Internet Control Message Protocol (ICMP) type:

  Following are the supported ICMP types:

  - **0**-**65535**—Port number.
  - **alternate-address**—Alternate address.
  - **conversion-error**—Datagram conversion.
  - **echo**—Echo (ping).
  - **echo-reply**—Echo reply.
  - **information-reply**—Information replies.
  - **information-request**—Information requests.
  - **mask-reply**—Mask replies.

  - **mask-request**—Mask requests.
  - **mobile-redirect**—Mobile host redirect.
  - **parameter-problem**—All parameter problems.
  - **redirect**—All redirects.
  - **router-advertisement**—Router discovery advertise.
  - **router-solicitation**—Router discovery solicitations.
  - **source-quench**—Source quenches.
  - **time-exceeded**—All time exceededs.
  - **timestamp-reply**—Timestamp replies.
  - **timestamp-request**—Timestamp requests.
  - **traceroute**—Traceroute.
  - **unreachable**—All unreachables.

- **group-object** *nested-object-group-name*—Existing network object group (child) to be included in the current object group (parent).

  The type of child object group must match that of the parent (for example, if you are creating a network object group, you must specify another network object group as the child).

  You can use duplicated objects in an object group if it is because of the inclusion of group objects. For example, if object 1 is in both group A and group B, you can define a group C that includes both A and B. However, you cannot include a group object that causes the group hierarchy to become circular (for example, you cannot include group A in group B and then also include group B in group A).

  You can use an unlimited number of nested object groups (however, a maximum of two levels is recommended).

Use the **no** form of the command to delete the object group with the specified name. (You cannot delete an object group that is being used within an ACL or a CPL policy.)

Examples

This example shows how to create a service object group that matches protocol port 100 and any port greater than 200, except 300:

```
Router> enable
Router# configure terminal
Router(config)# object-group service my_service_object_group
Router(config-service-group)# eq 100
Router(config-service-group)# gt 200
Router(config-service-group)# neq 300
```

Related Commands

Command	Description
deny	Sets conditions in a named IP access list or OGACL that will deny packets.
ip access-group	Applies an ACL or OGACL to an interface or a service policy map.
ip access-list	Defines an IP access list or OGACL by name or number.
object-group network	Defines network object groups for use in OGACLs.
permit	Sets conditions in a named IP access list or OGACL that will permit packets.

Command	Description
show ip access-list	Displays the contents of IP access lists or OGACLs.
show object-group	Displays information about object groups that are configured

occur-at (ips-auto-update)

To define a preset time for which the Cisco IOS Intrusion Prevention System (IPS) automatically obtains updated signature information, use the **occur-at** command in IPS-auto-update configuration mode.

occur-at {[**monthly** | **weekly**] *day minutes hours*}

Syntax Description

monthly	Monthly update option in days of the month from 1 to 31, minutes from the top of the hour from 0 to 59 and hours of the day from 0 to 23, in which automatic signature updates occur.
weekly	Weekly update option in days of the week from 0 to 6, minutes from the top of the hour from 0 to 59 and hours of the day from 0 to 23, in which automatic signature updates occur.

Command Default

The default value is defined in the signature definition XML.

Command Modes

IPS-auto-update configuration (config-ips-auto-update)

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.4(22)T	The command was modified with the **monthly** and **weekly** keywords in Cisco IOS Release 12.4(22)T.

Usage Guidelines

Automatic signature updates allow users to override the existing IPS configuration and automatically keep signatures up to date on the basis of a preset time, which can be configured to a preferred setting.

Use the **ip ips auto-update** command to enable Cisco IOS IPS to automatically update the signature file on the system. Thereafter, issue the **occur-at** command to define how often the Cisco IOS IPS signature files should be automatically updated.

Examples

The following example shows how to configure automatic signature updates and set the frequency in which updates are made. In this example, the signature package file is pulled from the TFTP server at the third hour of the 5 day of the month, at the 56th minute of this hour.

Note Adjustments are made for months without 31 days and daylight savings time.

```
Router# clock set ?
    hh:mm:ss Current Time
Router# clock set 10:38:00 20 apr 2006
Router#
*Apr 20 17:38:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 10:37:55 MST
Thu Apr 20 2006 to 10:38:00 MST Thu Apr 20 2006, configured from console by cisco on
console.
```

```
Router(config)# ip ips auto-update
Router(config-ips-auto-update)# occur-at monthly 5 56 3
Router(config-ips-auto-update)# $s-auto-update/IOS_reqSeq-dw.xml
Router(config-ips-auto-update)#^Z
Router#
*May 4 2006 15:50:28 MST: IPS Auto Update: setting update timer for next update: 0 hrs 10
min
*May 4 2006 15:50:28 MST: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router#
Router# show ip ips auto-update

    IPS Auto Update Configuration
    URL : tftp://192.168.0.2/jdoe/ips-auto-update/IOS_reqSeq-dw.xml
    Username : not configured
    Password : not configured
    Auto Update Intervals
    minutes (0-59) : 56
    hours (0-23) : 3
    days of month (1-31) : 5
    days of week: (0-6) :
```

Related Commands

Command	Description
ip ips auto-update	Enables automatic signature updates for Cisco IOS IPS.
cisco	Enables automatic signature updates from Cisco.com.

ocsp url

To specify the URL of an online certificate status protocol (OCSP) server to override the OCSP server URL (if one exists) in Authority Info Access (AIA) extension of the certificate, use the **ocsp url** command in ca-trustpoint configuration mode. To disable the OCSP server, use the **no** form of this command.

ocsp url *url*

no ocsp url *url*

Syntax Description

url	All certificates associated with a configured trustpoint will be checked by the OCSP server at the specified HTTP URL.

Defaults

Uses the OCSP server URL in AIA extension of the certificate. If a URL does not exist, revocation check will fail.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.

Usage Guidelines

A central OCSP server can be configured to collect and update certificate revocation lists (CRLs) from different certification authority (CA) servers. Thus, the devices within the network can rely on the OCSP server to check the certificate status without retrieving and caching each CRL for every device.

Examples

The following example shows how to configure your router to use the OCSP server at the HTTP URL "http://myocspserver:81." If the server is down, revocation check will be ignored.

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# ocsp url http://myocspserver:81
Router(ca-trustpoint)# revocation-check ocsp none
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the CA that your router should use.
revocation-check	Checks the revocation status of a certificate.

on

To specify the location where Rivest, Shamir, and Adelman (RSA) keys will be generated upon initial auto enrollment, use the **on** command in ca-trustpoint configuration mode.

on *devicename:*

Syntax Description

devicename:	Specifies the RSA key storage device.

Command Default

Keys are generated and stored in NVRAM.

Command Modes

Ca-trustpoint

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Locations that may be specified include a USB token, local disk, or NVRAM.

A USB token may be used as a cryptographic device in addition to a storage device. Using a USB token as a cryptographic devices allows RSA operations such as key generation, signing, and authentication to be performed on the token. Private keys are not distributed and remain on the token by default, however you may configure the private key storage location.

Keys that reside on a USB token, or on-token keys, are saved to persistent token storage when they are generated. Key deletion will remove the on-token keys from persistent storage immediately. (Keys that do not reside on a token are saved to or deleted from non-token storage locations only when the **write memory** or similar command is issued.)

Examples

The following example shows the configuration for the "mytp-A" certificate server and its associated trustpoint, where RSA keys generated by the initial auto enrollment for the trustpoint will be stored on a USB token, "usbtoken0":

```
crypto pki server mytp-A
   database level complete
   issuer-name CN=company, L=city, C=country
   grant auto
! Specifies that certificate requests will be granted automatically.
!

crypto pki trustpoint mytp-A
   revocation-check none
   rsakeypair myTP-A
   storage usbtoken0:
! Specifies that keys will be stored on usbtoken0:.
   on usbtoken0:
! Specifies that keys generated on initial auto enroll will be generated on and stored on
! usbtoken0:
```

Related Commands

Command	Description
crypto key generate rsa	Generates RSA key pairs.
crypto key import rsa	Imports RSA key pairs.
crypto pki trustpoint	Declares the trustpoint that the router will use.

one-minute

To define the number of new unestablished sessions that will cause the system to start deleting half-open sessions and stop deleting half-open sessions, use the **one-minute** command in parameter-map type inspect configuration mode. To disable the value, use the **no** form of this command.

one-minute {**low** *number-of-connections* | **high** *number-of-connections*}

no one-minute {**low** *number-of-connections* | **high** *number-of-connections*}

Syntax Description

low *number-of-connections*	Number of new unestablished sessions that will cause the system to stop deleting half-open sessions.
high *number-of-connections*	Number of new unestablished sessions that will cause the system to start deleting half-open sessions.

Command Default

None

Command Modes

Parameter-map type inspect configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

When you are configuring an inspect type parameter map, you can enter the **one-minute** subcommand after you enter the **parameter-map type inspect** command.

Enter the **one-minute** command twice; once to specify a high number at which the system will start deleting half-open sessions, and once to specify a low number at which the system will stop deleting half-open sessions.

For more detailed information about creating a parameter map, see the **parameter-map type inspect** command.

Examples

The following example causes the system to start deleting half-open sessions when there are 300 unestablished sessions, and to stop deleting half-open sessions when there are 400 unestablished systems:

```
parameter-map type inspect internet-policy
 one minute high 400
 one minute low 300
```

Related Commands

Command	Description
ip inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ip inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

outgoing

To configure filtering for outgoing export traffic, use the **outgoing** command in router IP traffic export (RITE) configuration mode. To disable filtering for outgoing traffic, use the **no** form of this command.

outgoing {**access-list** {*standard* | *extended* | *named*} | **sample one-in-every** *packet-number*}

no outgoing {**access-list** {*standard* | *extended* | *named*} | **sample one-in-every** *packet-number*}

Syntax Description

access-list {*standard* | *extended* | *named*}	An existing numbered (standard or extended) or named access control list (ACL). **Note** The filter is applied only to exported traffic.
sample one-in-every *packet-number*	Export only one packet out of every specified number of packets. Valid range for the *packet-number* argument is 2 to 2147483647 packets.

Defaults

If this command is not enabled, outgoing IP traffic is not exported.

Command Modes

RITE configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

When configuring a network device for IP traffic export, you can issue the **outgoing** command to filter unwanted outgoing traffic via the following methods:

- ACLs, which accept or deny an IP packet for export
- Sampling, which allows you to export one in every few packets in which you are interested. Use this option when it is not necessary to export all incoming traffic. Also, sampling is useful when a monitored ingress interface can send traffic faster than the egress interface can transmit it.

Note If you issue this command, you must also issue the **bidirectional** command, which enables outgoing traffic to be exported. However, only routed traffic (such as passthrough traffic) is exported; that is, traffic that originates from the network device is not exported.

Examples

The following example shows how to configure the profile “corp1,” which will send captured IP traffic to host “00a.8aab.90a0” at the interface “FastEthernet 0/1.” This profile is also configured to export one in every 50 packets and to allow incoming traffic only from the ACL “ham_ACL.”

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
```

```
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```

Related Commands

Command	Description
bidirectional	Enables incoming and outgoing IP traffic to be exported across a monitored interface.
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.
incoming	Configures filtering for incoming IP traffic.

parameter

To specify parameters for an enrollment profile, use the **parameter** command in ca-profile-enroll configuration mode. To disable specified parameters, use the **no** form of this command.

parameter *number* {**value** *value* | **prompt** *string*}

no parameter *number* {**value** *value* | **prompt** *string*}

Syntax Description

number	User parameters. Valid values range from 1 to 8.
value *value*	To be used if the parameter has a constant value.
prompt *string*	To be used if the parameter is supplied after the **crypto ca authenticate** command or the **crypto ca enroll** command has been entered. **Note** The value of the *string* argument does not have an effect on the value that is used by the router.

Defaults

No enrollment profile parameters are specified.

Command Modes

Ca-profile-enroll configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

The **parameter** command can be used within an enrollment profile after the **authentication command** command or the **enrollment command** has been enabled.

Examples

The following example shows how to specify parameters for the enrollment profile named “E”:

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial

crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
authentication command	Specifies the HTTP command that is sent to the CA for authentication.
crypto ca profile enrollment	Defines an enrollment profile.
enrollment command	Specifies the HTTP command that is sent to the CA for enrollment.

parameter-map type

To create or modify a parameter map, use the **parameter-map type** command in global configuration mode. To delete a parameter map from the configuration, use the **no** form of this command.

parameter-map type {**inspect** | **urlfilter** | **protocol-info** | **consent**} *parameter-map-name*

no parameter-map type {**inspect** | **urlfilter** | **protocol-info** | **consent**} *parameter-map-name*

Syntax Description

inspect	Defines an inspect type parameter map, which configures connection thresholds, timeouts, and other parameters pertaining to the **inspect** action.
urlfilter	Defines a URL-filter-specific parameter map.
protocol-info	Defines an application-specific parameter map. **Note** Protocol-specific parameter maps can be created only for Instant Messenger (IM) applications (AOL, I Seek You (ICQ), MSN Messenger, Yahoo Messenger and Windows Messenger).
consent	Defines an authentication proxy consent parameter map.
parameter-map-name	Name of the parameter map.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(9)T	The **protocol-info** keyword was added.
12.4(15)T	The **consent** keyword was added.
12.4(20)T	Support for ICQ and Windows Messenger was added.

Usage Guidelines

A parameter map allows you to specify parameters that control the behavior of actions and match criteria specified under a policy map and a class map, respectively.

There are currently four types of parameter maps:

- Inspect parameter map

  An inspect parameter map is optional. If you do not configure a parameter map, the software uses default parameters. Parameters associated with the inspect action apply to all nested actions (if any). If parameters are specified in both the top and lower levels, those in the lower levels override those in the top levels.

- URL filter parameter map

  A parameter map is required for URL filtering (via the URL filter action in a Layer 3 or Layer 4 policy map and the URL filter parameter map).

- Protocol-specific parameter map

  A parameter map is required for an IM application (Layer 7) policy map.
- Authentication proxy consent-specific parameter map.

Examples

The following example shows how to configure an IM-based firewall policy. In this example, all Yahoo Messenger and ICQ traffic is allowed to pass through, while all MSN Messenger, AOL and Windows Messenger traffic is blocked. Also, parameter maps are defined to control all Yahoo Messenger and ICQ traffic on a more granular level.

```
!
!
parameter-map type protocol-info ymsgr-servers
 server name messenger.yahoo.akadns.net
 server name .*.yahoo.com snoop
 server ip 192.0.2.100
 server ip range 192.0.2.115 192.0.2.180
parameter-map type protocol-info icq-servers
 server name login.oscar.aol.com
 server name .*.aol.com snoop
 server ip 192.0.2.200
 server ip range 192.0.2.215 192.0.2.230
!
!
class-map type inspect match-all l4-cmap-ymsgr
 match protocol ymsgr ymsgr-servers
class-map type inspect ymsgr match-any l7-cmap-ymsgr
 match  service text-chat
class-map type inspect match-all l4-cmap-icq
 match protocol icq icq-servers
class-map type inspect icq match-any l7-cmap-icq
 match  service text-chat
 match  service any
!
!
policy-map type inspect im l7-pmap-ymsgr
 class type inspect ymsgr l7-cmap-ymsgr
  allow
  log
policy-map type inspect im l7-pmap-icq
 class type inspect icq l7-cmap-icq
  allow
  log
policy-map type inspect to_internet
 class type inspect l4-cmap-ymsgr
  inspect
  service-policy im l7-pmap-ymsgr
 class type inspect l4-cmap-icq
  inspect
  service-policy im l7-pmap-icq
 class class-default
  drop
!
!
```

The following example shows a typical URL filter parameter map configuration:

```
parameter-map type urlfilter eng-filter-profile
 server vendor n2h2 172.16.1.2 port 3128 outside log timeout 10 retrans 6
 max-request 80
 max-resp-pak 200
```

```
 cache 200
 exclusive-domain permit cisco.com
 exclusive-domain deny gaming.com
```

The following example shows a sample inspect type parameter map configuration:

```
parameter-map type inspect eng_network_profile
 audit-trail on
 alert off
 max-incomplete low 2000
 max-incomplete high 3000
 one-minute low 5000
 one-minute high 8000
 udp idle-time 75
 dns-timeout 25
 tcp idle-time 90
 tcp finwait-time 20
 tcp synwait-time 10
 tcp block-non-session
 tcp max-incomplete host 2000 block-time 120
```

The following example shows how to define the consent-specific parameter map "consent_parameter_map" and a default consent parameter map:

```
parameter-map type consent consent_parameter_map
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity consent_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
parameter-map type consent default
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity test_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
```

parameter-map type inspect

To configure an inspect type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action, use the **parameter-map type inspect** command in global configuration mode. To delete an inspect type parameter map, use the **no** form of this command.

parameter-map type inspect {*parameter-map-name* | **global** | **default**}

no parameter-map type inspect {*parameter-map-name* | **global** | **default**}

Syntax Description

parameter-map-name	Name of the inspect parameter map.
global	Defines a global inspect parameter map.
default	Defines a default inspect parameter map.

Command Default

No inspect type parameter maps are set.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.1(1)T	The keywords **global** and **default** were added.

Usage Guidelines

After you enter the **parameter-map type inspect** command, you can enter the following commands in parameter-map type inspect configuration mode:

- **alert** {**on** | **off**}

  Turns on Cisco IOS stateful packet inspection alert messages.

- **audit-trail** {**on** | **off**}

  Turns audit trail messages on or off.

- **dns-timeout** *seconds*

  Specifies the Domain Name System (DNS) idle timeout.

- **icmp idle-timeout** *seconds*

  Configures the timeout for Internet Control Message Protocol (ICMP) sessions.

- **max-incomplete** {**low** | **high**} *number-of-connections*

  Defines the number of existing half-open sessions that will cause the software to start and stop deleting half-open sessions.

- **one-minute** {**low** | **high**} *number-of-connections*

  Defines the rate of new half-open session initiation in one minute that will cause the system to start deleting half-open sessions and stop deleting half-open sessions.

- **tcp finwait-time** *seconds*

  Specifies how long a TCP session will be managed after the Cisco IOS firewall detects a FIN-exchange.

- **tcp idle-time** *seconds*

  Configures the timeout for TCP sessions.

- **tcp max-incomplete host** *threshold* [**block-time** *minutes*}

  Specifies threshold and blocking time values for TCP host-specific denial-of-service (DOS) detection and prevention.

- **tcp synwait-time** *seconds*

  Specifies how long the software will wait for a TCP session to reach the established state before dropping the session.

- **udp idle-time** *seconds*

  Configures the timeout of User Datagram Protocol (UDP) sessions going through the firewall.

For more detailed information about these commands, see their individual command descriptions.

Examples

The following example shows a sample inspect parameter map with the Cisco IOS stateful packet inspection alert messages enabled:

```
parameter-map type inspect eng-network-profile
 alert on
```

The following example shows a sample inspect type parameter map configuration:

```
parameter-map type inspect eng_network_profile
 audit-trail on
 alert on
 max-incomplete low unlimited
 max-incomplete high unlimited
 one-minute low unlimited
 one-minute high unlimited
 udp idle-time 30
 icmp idle-time 10
 dns-timeout 5
 tcp idle-time 3600
 tcp finwait-time 5
 tcp synwait-time 30
 tcp block-non-session
 tcp max-incomplete host 1-2147483647 block-time unlimited
 sessions maximum:2147483647
```

Related Commands

Command	Description
alert	Turns on Cisco IOS stateful packet inspection alert messages.
audit-trail	Turns audit trail messages on and off.
dns-timeout	Specifies the DNS idle timeout.
icmp idle-timeout	Configures the timeout for ICMP sessions.
inspect	Enables Cisco IOS stateful packet inspection.

Command	Description
max-incomplete	Defines the number of existing half-open sessions that will cause the software to start and stop deleting half-open sessions.
one-minute	Defines the number of new unestablished sessions that will cause the system to start deleting half-open sessions and stop deleting half-open sessions.
tcp finwait-time	Specifies how long a TCP session will be managed after the Cisco IOS firewall detects a FIN-exchange.
tcp idle-time	Configures the timeout for TCP sessions.
tcp max-incomplete host	Specifies threshold and blocking time values for TCP host-specific denial-of-service (DOS) detection and prevention.
tcp synwait-time	Specifies how long the software will wait for a TCP session to reach the established state before dropping the session.
udp idle-time	Configures the timeout of UDP sessions going through the firewall.

parameter-map type protocol-info

To create or modify a protocol-specific parameter map and enter parameter-map type configuration mode, use the **parameter-map type protocol-info** command in global configuration mode. To delete a protocol-specific parameter map from the configuration, use the **no** form of this command.

parameter-map type protocol-info [**msrpc** | **sip** | **stun-ice**] *parameter-map-name*

no parameter-map type protocol-info [**msrpc** | **sip** | **stun-ice**] *parameter-map-name*

Syntax Description

msrpc	(Optional) Defines a Microsoft Remote Procedure Call (MSRPC) protocol-info parameter map.
sip	(Optional) Defines a Session Initiation Protocol (SIP) protocol-info parameter map.
stun-ice	(Optional) Defines a Session Traversal Utilities for Network Address Translation (NAT) and Interactive Connectivity Establishment (STUN-ICE) protocol-info parameter map.
parameter-map-name	Name of the parameter map.

Command Default

No protocol-specific parameter maps are created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(11)T	This command was introduced.
15.0(1)M	This command was modified. The **sip** keyword was added.
15.1(4)M	This command was modified. The **msrpc** keyword was added.

Usage Guidelines

A protocol-specific parameter map allows you to specify the parameters that control the behavior of actions specified under a policy map and match criteria specified under a class map.

Protocol-specific parameter maps can be created for real-time voice, video, and text messaging applications (such as AOL, MSN Messenger, or Windows Messenger).

Examples

The following example shows a sample SIP protocol type parameter map configuration. In this example, the parameter map is configured to not open a media channel when attached to a SIP class map:

```
Router(config)# parameter-map type protocol-info sip pmap-sip
Router(config-profile)# disable open-media channel
```

The following example shows a sample STUN-ICE protocol type parameter map configuration. In this example, the parameter map is configured to not open a media channel when attached to a SIP class map:

```
Router(config)# parameter-map type protocol-info stun-ice
```

```
Router(config-profile)# disable open-media channel
Router(config-profile)# authorization agent-id 20 shared-secret 12345flower12345
cat-window 15
```

The following example shows how to configure an Instant Messaging-based firewall policy. In this example, all Yahoo Messenger and I Seek You (ICQ) traffic is allowed to pass through, while all MSN Messenger, AOL, and Windows Messenger traffic is blocked. Also, parameter maps are defined to control all Yahoo Messenger and ICQ traffic on a more granular level.

```
Router(config)# parameter-map type protocol-info ymsgr-servers
Router(config-profile)# server name messenger.yahoo.akadns.net
Router(config-profile)# server name .*.yahoo.com snoop
Router(config-profile)# server ip 192.0.2.100
Router(config-profile)# server ip range 192.0.2.115 192.0.2.180
Router(config-profile)# exit

Router(config)# parameter-map type protocol-info icq-servers
Router(config-profile)# server name login.oscar.aol.com
Router(config-profile)# server name .*.aol.com snoop
Router(config-profile)# server ip 192.0.2.200
Router(config-profile)# server ip range 192.0.2.215 192.0.2.230
Router(config-profile)# exit

Router(config)# class-map type inspect match-all l4-cmap-ymsgr
Router(config-cmap)# match protocol ymsgr ymsgr-servers
Router(config-cmap)# exit

Router(config)# class-map type inspect ymsgr match-any l7-cmap-ymsgr
Router(config-cmap)# match  service text-chat
Router(config-cmap)# exit

Router(config)# class-map type inspect match-all l4-cmap-icq
Router(config-cmap)# match protocol icq icq-servers
Router(config-cmap)# exit

Router(config)# class-map type inspect icq match-any l7-cmap-icq
Router(config-cmap)# match  service text-chat
Router(config-cmap)# match  service any
Router(config-cmap)# exit

Router(config)# policy-map type inspect im l7-pmap-ymsgr
Router(config-pmap)# class type inspect ymsgr l7-cmap-ymsgr
Router(config-pmap-c)# allow
Router(config-pmap-c)# log
Router(config-pmap-c)# exit

Router(config)# policy-map type inspect im l7-pmap-icq
Router(config-pmap)#class type inspect icq l7-cmap-icq
Router(config-pmap-c)# allow
Router(config-pmap-c)# log
Router(config-pmap-c)# exit

Router(config)# policy-map type inspect to_internet
Router(config-pmap)# class type inspect l4-cmap-ymsgr
Router(config-pmap-c)# inspect
Router(config-pmap-c)# service-policy im l7-pmap-ymsgr
Router(config-pmap-c)# exit

Router(config-pmap)# class type inspect l4-cmap-icq
Router(config-pmap-c)# inspect
Router(config-pmap-c)# service-policy im l7-pmap-icq
Router(config-pmap-c)# exit
```

```
Router(config-pmap)# class class-default
Router(config-pmap-c)# drop
```

Related Commands

Command	Description
disable open-media-channel	Prevents the creation of RTP or RTCP media channels when a SIP class map is used for SIP inspection.
parameter-map type inspect	Configures an inspect type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the inspect action.

parameter-map type inspect-vrf

To configure an inspect VPN Routing and Forwarding (VRF)-type parameter map, use the **parameter-map type inspect-vrf** command in global configuration mode. To delete an inspect VRF type parameter map, use the **no** form of this command.

parameter-map type inspect-vrf *vrf-pmap-name*

no parameter-map type inspect-vrf *vrf-pmap-name*

Syntax Description

vrf-pmap-name	Name of the parameter map.

Command Default

An inspect VRF-type parameter map is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Examples

The following example shows how to configure an inspect VRF-type parameter map named inspect-pmap:

```
Router(config)# parameter-map type inspect-vrf inspect-pmap
```

Related Commands

Command	Description
parameter-map type	Creates or modifies a parameter map.
show parameter-map type inspect-vrf	Displays information about the configured inspect VRF-type parameter maps.

parameter-map type inspect-zone

To configure an inspect zone-type parameter map, use the **parameter-map type inspect-zone** command in global configuration mode. To remove an inspect zone type parameter map, use the **no** form of this command.

parameter-map type inspect-zone *zone-pmap-name*

no parameter-map type inspect-zone *zone-pmap-name*

Syntax Description

zone-pmap-name	Name of the parameter map.

Command Default

Inspect zone-type parameter maps are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Examples

The following example shows how to create an inspect zone-type parameter map named zone-pmap:

```
Router(config)# parameter-map type inspect-zone zone-pmap
```

Related Commands

Command	Description
parameter-map type	Creates or modifies a parameter map.
show parameter-map type inspect-zone	Displays information about the configured inspect zone-type parameter maps.

parameter-map type regex

To configure a parameter-map type to match a specific traffic pattern, use the **parameter-map type regex** command in global configuration mode. To delete a parameter-map type with a regular expression (regex), use the **no** form of this command.

parameter-map type regex *parameter-map-name*

no parameter-map type regex

Syntax Description

parameter-map-name	Name of the parameter map. The name can be a maximum of 228 alphanumeric characters. **Note** Using blank spaces is not recommended. The system interprets the first blank space as the end of the parameter-map name unless the string contains blank spaces and is delimited by quotation marks.

Command Default

A regex parameter map is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

You can enter a regex to match text strings either literally as an exact string or by using metacharacters so that you can match multiple variants of a text string. You can use a regex to match the content of certain application traffic; for example, you can match a uniform resource identifier (URI) string inside an HTTP packet using the **match request regex** command under an HTTP inspection class map.

Use Ctrl-V to ignore all of the special characters in the command line interface (CLI), such as a question mark (?) or a tab. For example, type **d**[**Ctrl-V**]**g** to enter **d?g** in the configuration.

Table 44 lists the metacharacters that have special meanings.

Table 44 regex Metacharacters

Character	Description	Notes
.	Dot	Matches any single character. For example, **d.g** matches dog, dag, dtg, and any word that contains those characters.
(*xxx*)	Subexpression	A subexpression segregates characters from surrounding characters, so that you can use other metacharacters on the subexpression. For example, **d(o|a)g** matches dog and dag, but **do|ag** matches do and ag. A subexpression can also be used with repeat quantifiers to differentiate the characters meant for repetition. For example, **ab(xy){3}z** matches abxyxyxyz.
|	Alternation	Matches either expression that it separates. For example, **dog|cat** matches dog or cat.
?	Question mark	A quantifier that indicates that there are 0 or 1 of the previous expression. For example, **lo?se** matches lse or lose. **Note** You must enter Ctrl-V and then the question mark or else the help function is invoked.
*	Asterisk	A quantifier that indicates that there are 0, 1 or any number of the previous expression. For example, **lo*se** matches lse, lose, loose, and so on.
+	Plus	A quantifier that indicates there is at least one occurrence of the previous expression. For example, **lo+se** matches lose and loose, but not lse.
{*x*}	Repeat quantifier	Repeat exactly *x* times. For example, **ab(xy){3}z** matches abxyxyxyz.
{*x*,}	Minimum repeat quantifier	Repeat at least *x* times. For example, **ab(xy){2,}z** matches abxyxyz, abxyxyxyz, and so on.
[*abc*]	Character class	Matches any character in the brackets. For example, [**abc**] matches a, b, or c.
[^*abc*]	Negated character class	Matches a single character that is not contained within the brackets. For example, [**^abc**] matches any character other than a, b, or c; and [**^A-Z**] matches any single character that is not an uppercase letter.
[*a-c*]	Character range class	Matches any character in the range. [**a-z**] matches any lowercase letter. You can mix characters and ranges; for example, [**abcq-z**] matches a, b, c, q, r, s, t, u, v, w, x, y, z, and so does [**a-cq-z**]. **Note** The dash (-) character is literal only if it is the last or the first character within the brackets, [**abc-**] or [**-abc**].
" "	Quotation marks	Preserves trailing or leading spaces in the string. For example, **"test"** preserves the leading space when it looks for a match.

Table 44 regex Metacharacters (continued)

Character	Description	Notes
^	Caret	Specifies the beginning of a line.
\	Escape character	When preceding a literal character, matches a literal character. For example, \[matches the left square bracket.
char	Character	When character is not a metacharacter, matches the literal character.
\r	Carriage return	Matches a carriage return 0x0d.
\n	New line	Matches a new line 0x0a.
\t	Tab	Matches a tab 0x09.
\f	Formfeed	Matches a form feed 0x0c.
\x*nn*	Escaped hexadecimal number	Matches an ASCII character using hexadecimal numbers (exactly two digits).
nnn	Escaped octal number	Matches an ASCII character as an octal number (exactly three digits). For example, the character 040 represents a space.

Examples

The following example configures and applies a regex parameter map to an HTTP application firewall parameter-map type whose URI matches any of the following regular expressions:

- ".*cmd.exe"
- ".*money"
- ".*shopping"

```
Router# configure terminal
Router(config)# parameter-map type regex uri-regex-cm
Router(config-profile)# pattern ".*cmd.exe"
Router(config-profile)# pattern ".*money"
Router(config-profile)# pattern ".*shopping"
Router(config-profile)# exit

Router(config)# class-map type inspect http uri-check-cm
Router(config-cmap)# match request uri regex uri-regex-cm
Router(config-cmap)# exit

Router(config)# policy-map type inspect http uri-check-pm
Router(config-pmap)# class type inspect http uri-check-cm
Router(config-pmap-c)# reset
```

The following example configures a regex parameter map whose case-insensitive pattern matches multiple variants of the string "hello":

```
Router# configure terminal
Router(config)# parameter-map type regex body_regex
Router(config-profile)# pattern ".*[Hh][Ee][Ll][Ll][Oo]"
Router(config-profile)# end
```

Related Commands

Command	Description
class-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect type class map.
class type inspect	Specifies the traffic (class) on which an action is to be performed.
match request regex	Configures an HTTP firewall policy to permit or deny HTTP traffic on the basis of request messages whose URI or arguments (parameters) match a defined regular expression.
parameter-map type	Creates or modifies a parameter map.
policy-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect type policy map.

parameter-map type trend-global

To create or modify the parameter map for global parameters associated with a Trend Router Provisioning Server (TRPS) and to place the system in parameter map configuration mode, use the **parameter-map type trend-global** command in global configuration mode. To delete the global parameters associated with a TRPS from the configuration, use the **no** form of this command.

parameter-map type trend-global *parameter-map-name*

no parameter-map type trend-global *parameter-map-name*

Syntax Description

parameter-map-name	Name of the parameter map for the global parameters associated with the TRPS.

Command Default

No parameter map for the global TRPS parameters is created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
15.1(2)T	This command was modified. The **pipeline**, **on**, and **off** keywords were added.

Usage Guidelines

Use the **parameter-map type trend-global** command to specify global parameters for the TRPS. You can specify only one trend-global parameter map on the system. To specify per-policy parameters, use the **parameter-map type urlfpolicy** command.

When you create or modify a global TRPS parameter map, use the following commands in parameter map configuration mode to set the values for the global TRPS parameters:

- **alert** {**on** | **off**}—Turns on or off URL-filtering server alert messages that are displayed on the console. The default is **on**.
- **cache-entry-lifetime** *hours*—Specifies how long, in hours, an entry remains in the cache table. Cache entries remain in the table until the cache-entry-lifetime value for the entry expires or until the cache is full, whichever occurs first. When the cache is full, the entry is removed to make room for subsequent entries. The range is from 1 to 120. The default is 24.
- **cache-size maximum-memory** *kilobyte*—Specifies the maximum size of the categorization cache, in kilobytes. The range is from 0 to 128000. The default is 256.
- **exit**—Exits from the parameter map.
- **no**—Negates or sets default values for a command.

- **server** {*server-name* | *ip-address*} [**http-port** *port-number*] [**https-port** *port-number*] [**retrans** *retransmission-count*] [**timeout** *seconds*] [**pipeline** {**on** | **off**}]—Specifies information about the TRPS. Use the server command in profile configuration mode.
  - **http-port** *port-number*—Specifies the HTTP port that is listening for requests. The range is from 1 to 65535. The default is 80.
  - **https-port** *port-number*—Specifies the HTTPS port that is listening for secure HTTP requests. The range is from 1 to 65535. The default is 443.
  - **pipeline** {**on** | **off**}—Turns on or off the TRPS pipeline requests. The default is **on**.
  - **retrans** *retransmission-count*—Specifies the number of times the router retransmits the lookup request when a response is not received from the TRPS. The range is from 1 to 5. The default is 3.
  - **server** {*server-name* | *ip-address*}—Specifies the domain name or the IP address of the server. The default is trps.trendmicro.com.
  - **timeout** *seconds*—Specifies the number of seconds that the router waits for a response from the TRPS. The range is from 1 to 300. The default is 60.

Examples

The following shows an example of how to specify global TRPS parameters in a parameter map named global-parameter-map:

```
parameter-map type trend-global global-parameter-map
 server server.example.com retrans 5 timeout 200
 cache-size maximum-memory 128000
 cache-entry-lifetime 1
```

Related Commands

Command	Description
alert	Turns on or off URL-filtering system alert messages that are displayed on the console.
cache-entry lifetime	Specifies how long an entry remains in the cache table.
cache-size maximum-memory	Specifies the size of the categorization cache.
parameter-map type urlfpolicy	Specifies per-policy URL filtering parameters.
server	Specifies information about the TRPS.

parameter-map type urlfilter

Note This command is hidden in releases later than Cisco IOS Release 12.4(20)T, but it continues to work. The **parameter-map type urlfpolicy** command can also be used. This command is used to create URL filtering parameters for local, trend, Websense Internet filtering, and the N2H2 Internet blocking program. We recommend the use of the URL filter policy rather than the URL filter action for Cisco IOS Release 12.4(20)T. All the use-cases supported by URL filter as an action are also supported by URL filter policy.

To create or modify a parameter map for URL filtering parameters, use the **parameter-map type urlfilter** command in global configuration mode. To delete a URL filter parameter map, use the **no** form of this command.

parameter-map type urlfilter *parameter-map-name*

no parameter-map type urlfilter *parameter-map-name*

Syntax Description

parameter-map-name	Name of the URL parameter map.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was removed.

Usage Guidelines

When you are creating or modifying a URL parameter map, you can enter the following subcommands after you enter the **parameter-map type urlfilter** command. For more detailed information about the subcommands, see their individual command descriptions by going to the "Command Reference" section on page 45.

- **alert** {**on** | **off**}

  Turns on or off URL-filtering system alert messages that are displayed on the console.

- **allow-mode** {**on** | **off**}

  Turns on or off the default mode (allow mode) of the filtering algorithm.

- **audit-trail** {**on** | **off**}

  Turns on or off the logging of URL information into the syslog server or router.

- **cache** *number-of-entries*

  Configures cache parameters.

- **exclusive-domain** {**deny** | **permit**} *domain-name*

  Adds or removes a domain name to or from the exclusive domain list so that the Cisco IOS firewall does not have to send lookup requests to the vendor server.

- **max-request** *number-of-requests*

  Specifies the maximum number of outstanding requests that can exist at any given time.

- **max-resp-pak** *number-of-responses*

  Specifies the maximum number of HTTP responses that the Cisco IOS firewall can keep in its packet buffer.

- **server vendor** {**n2h2** | **websense**} {*ip-address* | *hostname* [**port** *port-number*]} [**outside**] [**log**] [**retrans** *retransmission-count*] [**timeout** *seconds*]

  Specifies a vendor server for URL filtering.

- **source-interface** *interface-name*

  Specifies the interface whose IP address will be used as the source IP address while making a TCP connection to the URL filter server (websense or N2h2).

Examples

The following example shows a sample URL parameter map:

```
parameter-map type urlfilter eng-network-profile
 server vendor n2h2 10.64.64.22 port 4128 outside retrans 4 timeout 8
```

The following example shows a typical URL filter configuration:

```
parameter-map type urlfilter eng-network-profile
 server vendor n2h2 10.64.65.22 port 3128 outside log retrans 6 timeout 10
 max-request 80
 max-resp-pak 200
 cache 200
 exclusive-domain permit cisco.com
 exclusive-domain deny gaming.com
```

Related Commands

Command	Description
alert	Turns on or off URL-filtering system alert messages that are displayed on the console.
allow-mode	Turns on or off the default mode (allow mode) of the filtering algorithm.
audit-trail	Turns on or off the logging of URL information into the syslog server or router.
cache	Configures cache parameters.
exclusive-domain	Adds or removes a domain name to or from the exclusive domain list so that the Cisco IOS firewall does not have to send lookup requests to the vendor server.
max-request	Specifies the maximum number of outstanding requests that can exist at any given time.
max-resp-pak	Specifies the maximum number of HTTP responses that the Cisco IOS firewall can keep in its packet buffer.
server vendor	Specifies a vendor server for URL filtering.

parameter-map type urlfpolicy

To create or modify a parameter map for a URL filtering policy and to place the system in parameter map configuration mode, use the **parameter-map type urlfpolicy** command in global configuration mode. To delete the parameter map for a URL filtering policy from the configuration, use the **no** form of this command.

parameter-map type urlfpolicy {**local** | **trend** | **n2h2** | **websense**} *parameter-map-name*

no parameter-map type urlfpolicy {**local** | **trend** | **n2h2** | **websense**} *parameter-map-name*

Syntax Description

local	Specifies that the parameters are for a local URL filtering policy. See Table 45 for more information.
trend	Specifies that the parameters are for a Trend Micro URL filtering policy. See Table 46 for more information.
n2h2	Specifies that the parameters are for a SmartFilter (previously N2H2) URL filtering policy. See Table 47 for more information.
websense	Specifies that the parameters are for a Websense URL filtering policy. See Table 47 for more information.
parameter-map-name	The name of the parameter map for a URL filtering policy.

Command Default

No parameter maps for a URL filtering policy are created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **parameter-map type urlfpolicy** command to create a parameter map for a URL filtering policy. The commands that you use to specify the parameters for a filtering policy depend on the URL filtering server you are using.

Table 45 defines the parameters for a local URL filtering policy.

Table 46 defines the per-policy parameters for a Trend Micro URL filtering policy. These parameters are in addition to the global Trend Micro policy parameters specified with the **parameter-map type trend-global** command.

Table 47 defines the per-policy parameters for SmartFilter (N2H2) and Websense URL filtering policies.

Table 45 Parameters for Local URL Filtering Policies

Syntax	Description
alert {**on** | **off**}	Turns on or off URL filtering alert messages that are displayed on the console. The default is **off**.
allow-mode {**on** | **off**}	Specifies whether to allow or block URL requests when the URL filtering process does not have connectivity to a URL filtering database. When **allow-mode** is **on**, all unmatched URL requests are allowed; when **off**, all unmatched URL requests are blocked. The default is **off**.
block-page {**message** *string* | **redirect-url** *url*}	Specifies the response to a blocked URL request. • **message** *string*—Specifies the message text to be displayed when a URL request is blocked. • **redirect-url** *url*—Specifies the URL of the web page to be displayed when a URL request is blocked.
exit	Exits from the parameter map.
no	Negates or sets default values for a command.

Table 46 Parameters for Trend Micro URL Filtering Policies

Syntax	Description
allow-mode {**on** | **off**}	Specifies whether to allow or block URL requests when the URL filtering process does not have connectivity to a URL filtering database. When **allow-mode** is **on**, all unmatched URL requests are allowed; when **off**, all unmatched URL requests are blocked. The default is **off**.
block-page {**message** *string* | **redirect-url** *url*}	Specifies the response to a blocked URL request. • **message** *string*—Specifies the message text to be displayed when a URL request is blocked. • **redirect-url** *url*—Specifies the URL of the web page to be displayed when a URL request is blocked.
exit	Exits from the parameter map.
max-request *number-requests*	Specifies the maximum number of pending requests. The range is from 1 to 2147483647. The default is 1000.
max-resp-pak *number-responses*	Specifies the number of HTTP responses that can be buffered. The range is from 0 and 20000. The default is 200.
no	Negates or sets default values for a command.
truncate hostname	Specifies that URLs be truncated at the end of the domain name.

Table 47 Parameters for SmartFilter and Websense URL Filtering Policies

Syntax	Description
alert {**on** | **off**}	Turns on or off URL filtering alert messages that are displayed on the console. The default is **off**.
allow-mode {**on** | **off**}	Specifies whether to allow or block URL requests when the URL filtering process does not have connectivity to a URL filtering database. When **allow-mode** is **on**, all unmatched URL requests are allowed; when **off**, all unmatched URL requests are blocked. The default is **off**.
block-page {**message** *string* | **redirect-url** *url*}	Specifies the response to a blocked URL request. • **message** *string*—Specifies the message text to be displayed when a URL request is blocked. • **redirect-url** *url*—Specifies the URL of the web page to be displayed when a URL request is blocked.
cache-entry-lifetime *hours*	Specifies how long, in hours, an entry remains in the cache table. The default is 24.
cache-size maximum-entries *number-entries*	Specifies the maximum number of entries that can be stored in the categorization cache. The default is 5000.
exit	Exits from the parameter map.
max-request *number-requests*	Specifies the maximum number of pending requests. The range is from 1 to 2147483647. The default is 1000.
max-resp-pak *number-responses*	Specifies the number of HTTP responses that can be buffered. The range is from 0 and 20000. The default is 200.
no	Negates or sets default values for a command.
server {*server-name* | *ip-address*} [**outside**] [**port** *port-number*] [**retrans** *retransmission-count*] [**timeout** *seconds*]	Specifies the parameters for the URL filtering server. • **server** {*server-name* | *ip-address*} Specifies the domain name or the IP address of the URL filtering server. • **outside** Specifies whether the URL filtering server is outside the network. • **port** *port-number* Specifies the port that is listening for requests. The range is from 1 to 65535. The default is 80. • **retrans** *retransmission-count* Specifies the number of times the router retransmits the lookup request when a response is not received from the Trend Router Provisioning Server (TRPS). The range is from 1 to 5. The default is 3. • **timeout** *seconds* Specifies the number of seconds that the router waits for a response from the TRPS. The range is from 1 to 300. The default is 60.

Table 47 Parameters for SmartFilter and Websense URL Filtering Policies (continued)

Syntax	Description
source-interface *interface-name*	Specifies the interface whose IP address will be used as the source IP address when a TCP connection is established between the system and the URL filtering server.
truncate {hostname | script-options}	Specifies that URLs be truncated. • **hostname** Specifies that URLs be truncated at the end of the domain name. • **script-options** Specifies that URLs be truncated at the left-most question mark in the URL.
urlf-server-log {on | off}	Enables sending information about HTTP requests to the URL filtering server's log server. The information includes the URL, the hostname, the source IP address, and the destination IP address.

Examples

The following example shows a parameter map for a local URL filtering policy that does not send alert messages and displays the message "URL is blocked by local filters" when a URL is blocked:

```
parameter-map type urlfpolicy local local-parameter-map
 alert off
 block-page message "URL is blocked by local-filters"
```

The following example shows a configuration for global parameters and per-policy parameters for a Trend Micro URL filtering policy:

```
parameter-map type trend-global global-parameter-map
 server mytrps.trendmicro.com retrans 5 timeout 200
 cache-size maximum-memory 128000
 cache-entry-lifetime 1

parameter-map type urlfpolicy trend trend-parameter-map
 max-request 2147483647
 max-resp-pak 20000
 truncate hostname
 block-page message "group2 is blocked by trend"
```

The following example shows the configuration for per-policy parameters for a SmartFilter URL filtering policy:

```
parameter-map type urlfpolicy n2h2 n2h2-parameter-map
 server n2h2Server timeout 30
 max-request 2000
 max-resp-pak 2000
 source-interface Loopback0
 truncate script-parameters
 cache-size maximum-entries 100
 cache-entry-lifetime 1
 block-page redirect-url http://www.example.com
```

Related Commands

Command	Description
parameter-map type trend-global	Specifies the global parameters associated with Trend Micro URL filtering policies.

parameter-map type urlf-glob

To create or modify a parameter map used to specify a list of domains, URL keywords, or URL metacharacters that should be allowed or blocked by local URL filtering, use the **parameter-map type urlf-glob** command in global configuration mode. To delete the parameter map, use the **no** form of this command.

parameter-map type urlf-glob *parameter-map-name*

no parameter-map type urlf-glob *parameter-map-name*

Syntax Description

parameter-map-name	Name of the parameter map for a local URL filtering policy.

Command Default

No URL filtering parameter maps are created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **parameter-map type urlf-glob** command can be used to create a parameter map for trusted domains, a parameter map for untrusted domains, and a parameter map for URL keywords. The following sub-commands are available in parameter map configuration mode to specify matching parameters when the **parameter-map type urlf-glob** command is issued:

- **exit**—Exits from URL filtering parameter map configuration mode.
- **no**—Negates or sets default values for a command.
- **pattern** *expression*—Configures a matching pattern that refers to a domain name, URL keyword, URL metacharacter entry, or URL keyword and URL metacharacter combination. The characters /, {, and } are not allowed in the expression. The question mark (?) is not allowed because it is reserved for the help function in the command-line interface (CLI).

URL pattern matching is improved because the period (.) is interpreted as a dot, and not as a wildcard entry representing a single character, as is the case with regex regular expression pattern matching.

A URL keyword is a complete word that occurs after the domain name and that is between the forward slash (/) path delimiters. For example in the URL http://www.example.com/hack/123.html, only “hack” and “123.html” are treated as keywords. Anything in the host or domain name can be allowed or blocked using a domain name, and thus a URL keyword should be a word that comes after the domain name. The entire keyword in the URL must match the pattern. For example if you have **pattern** *hack*, the URL www.example.com/hacksite/123.html doesn't match the pattern. In order to match this URL, you must have *hacksite*.

URL metacharacters allow pattern matching of single characters or ranges of characters to URLs, similar to the way a UNIX style glob expression works. The URL metacharacters are presented in Table 48.

Table 48 URL Metacharacters for URL Pattern Matching

Character	Description
*	Asterisk—matches any sequence of 0 or more characters.
[*abc*]	Character class—matches any character in the brackets. The character matching is case sensitive. For example, [abc] matches a, b, or c.
[*a-c*]	Character range class. Matches any character in the range. The character matching is case sensitive. [a-z] matches any lowercase letter. You can mix characters and ranges; for example, [abcq-z] matches a, b, c, q, r, s, t, u, v, w, x, y, z, and so does [a-cq-z]. **Note** The dash (-) character is literal only if it is the last or the first character within the brackets, [abc-] or [-abc].
[*0-9*]	Numerical range class. Matches any number in the brackets. For example [0-9] matches 0, 1, 2, 3, 4, 5, 6, 7, 8, or 9.

URL metacharacters are combined with domain names and URL keywords for pattern matching. For example, **pattern** *.example.com will match the domain name www.example.com and **pattern** www.[ey]xample.com can be used to block both www.example.com and www.yxample.com. Also, **pattern** www.example[0-9][0-9].com can be used to block www.example01.com, www.example33.com, and www.example99.com. An example of combining a keyword and metacharacter for pattern matching is using **pattern** hack* to block www.example.com/hacksite/123.html.

Examples

The following shows an example of specifying the parameter map for trusted domains:

```
Router(config)# parameter-map type urlf-glob trusted-domain-param
Router(config-profile)# pattern www.example.com
Router(config-profile)# pattern *.example2.com
```

The following shows an example of a parameter map specifying keywords to be blocked:

```
Router(config)# parameter-map type urlf-glob keyword-param
Router(config-profile)# pattern example1
Router(config-profile)# pattern example3
```

The following shows an example of a parameter map specifying URL metacharacters to be blocked:

```
Router(config)# parameter-map type urlf-glob metacharacter-param
```

Related CommandsR

Command	Description
class-map type urlfilter	Creates a class map that specifies the traffic to which a URL filtering policy applies.
pattern (parameter-map)	Configures a matching pattern that specifies a list of domains, URL keywords, or URL metacharacters that should be allowed or blocked by local URL filtering.

parser view

To create or change a command-line interface (CLI) view and enter view configuration mode, use the **parser view** command in global configuration mode. To delete a view, use the **no** form of this command.

parser view *view-name*

no parser view *view-name*

Syntax Description

view-name	View name, which can include 1 to 30 alphanumeric characters. The *view-name* argument must not have a number as the first character; otherwise, you will receive the following error message: "Invalid view name."

Defaults

A CLI view does not exist.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

A CLI view is a set of operational commands and configuration capabilities that restrict user access to the CLI and configuration information; that is, a view allows users to define what commands are accepted and what configuration information is visible.

After you have issued the **parser view** command, you can configure the view via the **secret 5** command and the **commands** command.

To invoke the **parser view** command, the system of the user must be set to root view. The root view can be enabled via the **enable view** command.

Examples

The following example shows how to configure two CLI views, "first" and "second":

```
Router(config)# parser view first
00:11:40:%PARSER-6-VIEW_CREATED:view 'first' successfully created.
Router(config-view)# secret 5 firstpass
Router(config-view)# command exec include show version
Router(config-view)# command exec include configure terminal
Router(config-view)# command exec include all show ip
Router(config-view)# exit
Router(config)# parser view second
```

```
00:13:42:%PARSER-6-VIEW_CREATED:view 'second' successfully created.
Router(config-view)# secret 5 secondpass
Router(config-view)# command exec include-exclusive show ip interface
Router(config-view)# command exec include logout
Router(config-view)# exit
```

After you have successfully created a view, a system message such as the following will be displayed:

```
%PARSER-6-VIEW_CREATED: view ‘first’ successfully created.
```

After you have successfully deleted a view, a system message such as the following will be displayed:

```
%PARSER-6-VIEW_DELETED: view ‘first’ successfully deleted.
```

Related Commands

Command	Description
commands (view)	Adds commands to a CLI view.
secret 5	Associates a CLI view or a superview with a password.

parser view superview

To create a superview and enter view configuration mode, use the **parser view superview** command in global configuration mode. To delete a superview, use the **no** form of this command.

parser view *superview-name* **superview**

no parser view *superview-name* **superview**

Syntax Description

superview-name	Superview name, which can include 1 to 30 alphanumeric characters. The *superview-name* argument must not have a number as the first character.

Defaults

A superview does not exist.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

A superview consists of one or more command-line interface (CLI) views, which allow users to define what commands are accepted and what configuration information is visible. Superviews allow a network administrator to easily assign all users within configured CLI views to a superview instead of having to assign multiple CLI views to a group of users.

Superviews contain the following characteristics:

- A CLI view can be shared among multiple superviews.
- Commands cannot be configured for a superview; that is, you must add commands to the CLI view and add that CLI view to the superview.
- Users who are logged in to a superview can access all of the commands that are configured for any of the CLI views that are part of the superview.
- Each superview has a password that is used to switch between superviews or from a CLI view to a superview.

Adding CLI Views to a Superview

You can add a view to a superview only after a password has been configured for the superview (via the **secret 5** command). Thereafter, issue the **view** command in view configuration mode to add at least one CLI view to the superview.

Note Before adding a CLI view to a superview, ensure that the CLI views that are added to the superview are valid views in the system; that is, the views have been successfully created via the **parser view** command.

Examples

The following example shows how to create a superview (su_view1) and enter view configuration mode; two CLI views (view_one, view_two) are added to the superview also:

```
Router> enable view
Router# configure terminal
Router(config)# parser view su_view1 superview
Router(config-view)# secret 5 secret
Router(config-view)# view view_one
Router(config-view)# view view_two
```

Related Commands

Command	Description
parser view	Creates or changes a CLI view and enters view configuration mode.
secret 5	Associates a CLI view or a superview with a password.
view	Adds a normal CLI view to a superview.

pass

To allow packets to be sent to the router without being inspected, use the **pass** command in policy-map-class configuration mode.

pass

Syntax Description

This command has no arguments or keywords.

Command Default

Traffic is not passed; that is, it is dropped.

Command Modes

Policy-map-class configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use this command only after entering the **policy-map type inspect**, **class type inspect**, and **parameter-map type inspect** commands.

Examples

The following example specifies that policy map p1 will pass the traffic:

```
policy-map type inspect p1
 class type inspect c1
  pass
```

Related Commands

Command	Description
class type inspect	Specifies the traffic (class) on which an action is to be performed.
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
policy-map type inspect	Creates a Layer 3 or Layer 4 inspect type policy map.

passive

To move a group member directly into passive mode, use the **passive** command in crypto gdoi group configuration mode. To disable the passive mode setting, use the **no** form of this command.

passive

no passive

Syntax Description

This command has no arguments or keywords.

Command Default

The group member is in full crypto send and receive mode.

Command Modes

Crypto gdoi group configuration (crypto-gdoi-group)

Command History

Release	Modification
12.4(22)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

By using the **passive** command, you avoid having to use the **crypto gdoi gm ipsec direction inbound optional** privileged EXEC command, which is not persistent after a router reload and can be overriden by key server configuration from a rekey.

Examples

The following example shows that the group member group1 is being moved to passive mode:

```
crypto gdoi group group1
 identity 2345
 passive
 server address ipv4 10.34.255.57
```

Related Commands

Command	Description
crypto gdoi gm	Changes the IPsec SA status of group members.

password (ca-trustpoint)

To specify the revocation password for the certificate, use the **password** command in ca-trustpoint configuration mode. To erase any stored passwords, use the **no** form of this command.

password *string*

no password

Syntax Description

string	Name of the password.

Defaults

You are prompted for the password during certificate enrollment.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

Before you can issue the **password** command, you must enable the **crypto ca trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.

This command allows you to specify the revocation password for the certificate before actual certificate enrollment begins. The specified password is encrypted when the updated configuration is written to NVRAM by the router.

If this command is enabled, you will not be prompted for a password during certificate enrollment.

Examples

The following example shows how to specify the password “revokeme” for the certificate request:

```
crypto ca trustpoint trustpoint1
 enrollment url http://trustpoint1.example.com/
 subject-name OU=Spiral Dept., O=example1.com
 ip-address ethernet-0
 auto-enroll regenerate
 password revokeme
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

password (dot1x credentials)

To specify the password for an 802.1X credentials profile, use the **password** command in dot1x credentials configuration mode. To remove the password, use the **no** form of this command.

password [**0** | **7**] *password*

no password

Syntax Description

0	(Optional) A plain text password will follow. The default is 0.
7	(Optional) An encrypted password will follow. The default is 0.
password	The password.

Command Default

A password is not specified.

Command Modes

Dot1x credentials configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Before using this command, the **dot1x credentials** command must have been configured.

Examples

The following example shows which credentials profile should be used when configuring a supplicant. The password is “secret.”

```
dot1x credentials basic-user
 username router
 password secret
 description This credentials profile should be used for most configured ports
```

The credentials structure can be applied to an interface along with the **dot1x pae supplicant** command and keyword to enable supplicant functionality on that interface.

```
interface fastethernet 0/1
 dot1x credentials basic-user
 dot1x pae supplicant
```

Related Commands

Command	Description
dot1x credentials	Specifies the 802.1X credentials profile to be used.

password (line configuration)

To specify a password on a line, use the **password** command in line configuration mode. To remove the password, use the **no** form of this command.

password *password*

no password

Syntax Description

password	Character string that specifies the line password. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces, up to 80 characters. You cannot specify the password in the format number-space-anything. The space after the number causes problems. For example, hello 21 is a legal password, but 21 hello is not. The password checking is case sensitive. For example, the password Secret is different than the password secret.

Defaults

No password is specified.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When an EXEC process is started on a line with password protection, the EXEC prompts for the password. If the user enters the correct password, the EXEC prints its normal privileged prompt. The user can try three times to enter a password before the EXEC exits and returns the terminal to the idle state.

Examples

The following example removes the password from virtual terminal lines 1 to 4:

```
line vty 1 4
 no password
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.

password 5

Note Effective with Cisco IOS Release 12.3(14)T, this command is replaced by the **secret** command.

To associate a command-line interface (CLI) view or a superview with a password, use the **password 5** command in view configuration mode.

password 5 *password*

Syntax Description

password	Password for users to enter the CLI view or superview. A password can contain any combination of alphanumeric characters. **Note** The password is case sensitive.

Defaults

A user cannot access a CLI view or superview.

Command Modes

View configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.3(11)T	This command was enhanced to support superviews.
12.3(14)T	This command was replaced by the secret command.

Usage Guidelines

A user cannot access any commands within the CLI view or superview until the **password 5** command has been issued.

Examples

The following example show how to configure two CLI views, “first” and “second” and associate each view with a password:

```
Router(config)# parser view first
00:11:40:%PARSER-6-VIEW_CREATED:view 'first' successfully created.
Router(config-view)# password 5 firstpass
Router(config-view)# command exec include show version
Router(config-view)# command exec include configure terminal
Router(config-view)# command exec include all show ip
Router(config-view)# exit
Router(config)# parser view second
00:13:42:%PARSER-6-VIEW_CREATED:view 'second' successfully created.
Router(config-view)# password 5 secondpass
Router(config-view)# command exec include-exclusive show ip interface
Router(config-view)# command exec include logout
Router(config-view)# exit
```

Related Commands

Command	Description
parser view	Creates or changes a CLI view and enters view configuration mode.

password encryption aes

To enable a type 6 encrypted preshared key, use the **password encryption aes** command in global configuration mode. To disable password encryption, use the **no** form of this command.

password encryption aes

no password encryption aes

Syntax Description

This command has no arguments or keywords.

Defaults

Preshared keys are not encrypted.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

You can securely store plain text passwords in type 6 format in NVRAM using a command-line interface (CLI). Type 6 passwords are encrypted. Although the encrypted passwords can be seen or retrieved, it is difficult to decrypt them to find out the actual password. Use the **key config-key password-encryption** command with the **password encryption aes** command to configure and enable the password (symmetric cipher Advanced Encryption Standard [AES] is used to encrypt the keys). The password (key) configured using the **key config-key password-encryption** command is the master encryption key that is used to encrypt all other keys in the router.

If you configure the **password encryption aes** command without configuring the **key config-key password-encryption** command, the following message is printed at startup or during any nonvolatile generation (NVGEN) process, such as when the **show running-config** or **copy running-config startup-config** commands have been configured:

```
"Can not encrypt password. Please configure a configuration-key with 'key config-key'"
```

Note For Cisco 836 routers, please note that support for Advanced Encryption Standard (AES) is available only on IP plus images.

Changing a Password

If the password (master key) is changed, or reencrypted, using the **key config-key password-encryption** command), the list registry passes the old key and the new key to the application modules that are using type 6 encryption.

Deleting a Password

If the master key that was configured using the **key config-key password-encryption** command is deleted from the system, a warning is printed (and a confirm prompt is issued) that states that all type 6 passwords will become useless. As a security measure, after the passwords have been encrypted, they will never be decrypted in the Cisco IOS software. However, passwords can be reencrypted as explained in the previous paragraph.

Caution If the password configured using the **key config-key password-encryption** command is lost, it cannot be recovered. The password should be stored in a safe location.

Unconfiguring Password Encryption

If you later unconfigure password encryption using the **no password encryption aes** command, all existing type 6 passwords are left unchanged, and as long as the password (master key) that was configured using the **key config-key password-encryption** command exists, the type 6 passwords will be decrypted as and when required by the application.

Storing Passwords

Because no one can "read" the password (configured using the **key config-key password-encryption** command), there is no way that the password can be retrieved from the router. Existing management stations cannot "know" what it is unless the stations are enhanced to include this key somewhere, in which case the password needs to be stored securely within the management system. If configurations are stored using TFTP, the configurations are not standalone, meaning that they cannot be loaded onto a router. Before or after the configurations are loaded onto a router, the password must be manually added (using the **key config-key password-encryption** command). The password can be manually added to the stored configuration but is not recommended because adding the password manually allows anyone to decrypt all passwords in that configuration.

Configuring New or Unknown Passwords

If you enter or cut and paste cipher text that does not match the master key, or if there is no master key, the cipher text is accepted or saved, but an alert message is printed. The alert message is as follows:

```
"ciphertext>[for username bar>] is incompatible with the configured master key."
```

If a new master key is configured, all the plain keys are encrypted and made type 6 keys. The existing type 6 keys are not encrypted. The existing type 6 keys are left as is.

If the old master key is lost or unknown, you have the option of deleting the master key using the **no key config-key password-encryption** command. Deleting the master key using the **no key config-key password-encryption** command causes the existing encrypted passwords to remain encrypted in the router configuration. The passwords will not be decrypted.

Examples

The following example shows that a type 6 encrypted preshared key has been enabled:

```
Router (config)# password encryption aes
```

Related Commands

Command	Description
key config-key password-encryption	Stores a type 6 encryption key in private NVRAM.
password logging	Provides a log of debugging output for a type 6 password operation.

password logging

To get a log of debugging output for a type 6 password operation, use the **password logging** command in global configuration mode. To disable the debugging, use the **no** form of this command.

password logging

no password logging

Syntax Description

This command has no arguments or keywords.

Defaults

Debug logging is not enabled.

Command Modes

Global Configuration #

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Examples

The following example shows that debug logging is configured:

```
Router# password logging
```

Related Commands

Command	Description
key config-key password-encryption	Stores an encryption key in private NVRAM.
password encryption aes	Enables a type 6 encrypted preshared key.

pattern (parameter-map)

To configure a matching pattern that specifies a list of domains, URL keywords, or URL metacharacters that should be allowed or blocked by local URL filtering, use the **pattern** command in parameter map configuration mode. To delete the parameter map, use the **no** form of this command.

pattern *expression*

no pattern *expression*

Syntax Description

expression	Matching pattern argument that can refer to a domain name, URL keyword, URL metacharacter entry, or URL keyword and URL metacharacter combination.

Command Default

No pattern is created for the parameter map.

Command Modes

Parameter map configuration (config-profile)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The matching pattern expression is configured for a parameter map created by the **parameter-map type urlf-glob** command. In the pattern expression, the characters /, {, and } are not allowed in the expression. The question mark (?) is not allowed because it is reserved for the help function in the command-line interface (CLI).

URL pattern matching is improved because the period (.) is interpreted as a dot, and not as a wildcard entry representing a single character, as is the case with regex regular expression pattern matching.

A URL keyword is a complete word that occurs after the domain name and that is between the forward slash (/) path delimiters. For example in the URL http://www.example.com/hack/123.html, only “hack” and “123.html” are treated as keywords. Anything in the host or domain name can be allowed or blocked using a domain name, and thus a URL keyword should be a word that comes after the domain name. The entire keyword in the URL must match the pattern. For example if you have **pattern** *hack*, the URL www.example.com/hacksite/123.html doesn't match the pattern. In order to match this URL, you must have *hacksite*.

URL metacharacters allow pattern matching of single characters or ranges of characters to URLs, similar to the way a UNIX style glob expression works. The URL metacharacters are presented in Table 48.

Table 49 URL Metacharacters for URL Pattern Matching

Character	Description
*	Asterisk—matches any sequence of 0 or more characters.
[*abc*]	Character class—matches any character in the brackets. The character matching is case sensitive. For example, [abc] matches a, b, or c.
[*a-c*]	Character range class. Matches any character in the range. The character matching is case sensitive. [a-z] matches any lowercase letter. You can mix characters and ranges; for example, [abcq-z] matches a, b, c, q, r, s, t, u, v, w, x, y, z, and so does [a-cq-z]. **Note** The dash (-) character is literal only if it is the last or the first character within the brackets, [abc-] or [-abc].
[*0-9*]	Numerical range class. Matches any number in the brackets. For example [0-9] matches 0, 1, 2, 3, 4, 5, 6, 7, 8, or 9.

URL metacharacters are combined with domain names and URL keywords for pattern matching. For example, **pattern** *.example.com will match the domain name www.example.com and **pattern** www.[ey]xample.com can be used to block both www.example.com and www.yxample.com. Also, **pattern** www.example[0-9][0-9].com can be used to block www.example01.com, www.example33.com, and www.example99.com. An example of combining a keyword and metacharacter for pattern matching is using **pattern** hack* to block www.example.com/hacksite/123.html.

Examples

The following shows an example of specifying the parameter map for trusted domains:

```
Router(config)# parameter-map type urlf-glob trusted-domain-param
Router(config-profile)# pattern www.example.com
Router(config-profile)# pattern *.example2.com
```

The following shows an example of a parameter map specifying keywords to be blocked:

```
Router(config)# parameter-map type urlf-glob keyword-param
Router(config-profile)# pattern example1
Router(config-profile)# pattern example3
```

The following shows an example of a parameter map specifying URL metacharacters to be blocked:

```
Router(config)# parameter-map type urlf-glob metacharacter-param
Router(config-profile)# pattern www.example[4-9].com
```

Related Commands

Command	Description
class-map type urlfilter	Creates a class map that specifies the traffic to which a URL filtering policy applies.
parameter-map type urlf-glob	Creates or modifies a parameter map used to specify a list of domains, URL keywords, or URL metacharacters that should be allowed or blocked by local URL filtering and enters parameter map configuration mode.

peer address ipv4

To configure a Group Domain of Interpretation (GDOI) redundant peer key server, use the **peer address ipv4** command in GDOI redundancy configuration mode. To remove the peer key server that was configured, use the **no** form of this command.

peer address ipv4 *ip-address*

no peer address ipv4 *ip-address*

Syntax Description

ip-address	IP address of the peer key server.

Command Default

(Redundancy does not function correctly if at least one peer is not configured under the local key server configuration on a key server.)

Command Modes

GDOI redundancy configuration (gdoi-coop-ks-config)

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

For redundancy between key servers to operate correctly, there have to be at least two key servers in a redundant group. Therefore, at least one other peer must be defined on a key server using the **peer address ipv4** command. The local key server sets up an Internet Key Exchange (IKE) session with the peer that is defined using this command and proceeds to communicate using IKE informational messages to complete the election process using the specified IP address of the peer.

Examples

The following example shows that two peer key servers have been configured: 10.41.2.5 and 10.33.5.6.

```
address ipv4 10.1.1.1
redundancy
 local priority 10
 peer address ipv4 10.41.2.5
 peer address ipv4 10.33.5.6
```

Related Commands

Command	Description
address ipv4	Sets the source address, which is used as the source for packets originated by the local key server.
local priority	Sets the local key server priority.

Command	Description
redundancy	Enters GDOI redundancy configuration mode and allows for key server redundancy.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

peer (IKEv2 keyring)

To define a peer or a peer group for the Internet Key Exchange Version 2 (IKEv2) keyring, use the **peer** command in IKEv2 keyring configuration mode. To remove the peer, use the **no** form of this command.

peer *name*

no peer *name*

Syntax Description

name	The peer name.

Command Default

A peer is not defined or configured.

Command Modes

IKEv2 keyring configuration (config-ikev2-keyring)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to define the name of a peer or peer group. This command enters IKEv2 keyring peer configuration mode. A peer subblock identifies a peer or peer-group using identity, hostname or address statements. A peer subblock must have atleast one statement identifying a peer or peer group. A peer subblock can have a single statement of each type identifying a peer or peer group. A peer subblock can have a single key or key-pair.

Examples

The following example shows how to configure an IKEv2 keyring with multiple peer subblocks:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(configikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# description peer1
Router(config-ikev2-keyring-peer)# address 10.0.0.1
Router(config-ikev2-keyring-peer)# pre-shared-key key-1

Router(configikev2-keyring)# peer peer2
Router(config-ikev2-keyring-peer)# description peer2
Router(config-ikev2-keyring-peer)# host peer1.example.com
Router(config-ikev2-keyring-peer)# pre-shared-key key-2

Router(configikev2-keyring)# peer peer3
Router(config-ikev2-keyring-peer)# description peer3
Router(config-ikev2-keyring-peer)# host peer3.example.com
Router(config-ikev2-keyring-peer)# identity key-id abc
Router(config-ikev2-keyring-peer)# address 10.0.0.3
Router(config-ikev2-keyring-peer)# pre-shared-key key-3
```

Related Commands

Command	Description
address (ikev2 keyring)	Specifies the IPv4 address or the range of the peers in IKEv2 keyring.
crypto ikev2 keyring	Defines an IKEv2 keyring.
description (ikev2 keyring)	Describes an IKEv2 peer or a peer group for the IKEv2 keyring.
hostname (ikev2 keyring)	Specifies the hostname for the peer in the IKEv2 keyring.
identity (ikev2 keyring)	Identifies the peer with IKEv2 types of identity.
pre-shared-key (ikev2 keyring)	Defines a preshared key for the IKEv2 peer.

permit

To set conditions in named IP access list or object group access control list (OGACL) that will permit packets, use the **permit** command in the appropriate configuration mode. To remove a condition from an IP access list or an OGACL, use the **no** form of this command.

permit *protocol* [*source-addr source-wildcard*] {**any** | **host** {*address* | *name*} | **object-group** *object-group-name*} {*destination-addr destination-wildcard* | **any** | **host** {*address* | *name*} | **object-group** *object-group-name*}[**dscp** *dscp-value* | **precedence** *precedence-value*] [**fragments** *fragment-value*] [**option** *option-value*] [**reflect** *access-list-name*] [**time-range** *time-range-value*] [**ttl** *match-value ttl-value* [*ttl-value*]] [**tos** *tos-value*] [**timeout** *max-time*]] [**log** [*log-value*] | **log-input** [*log-input-value*]]

no permit *protocol* [*source-addr source-wildcard*] {**any** | **host** {*address* | *name*} | **object-group** *object-group-name*} {*destination-addr destination-wildcard* | **any** | **host** {*address* | *name*} | **object-group** *object-group-name*}

permit {**tcp | udp**} {*source-addr source-wildcard* | **any** | **host** *source-addr* | **object-group** *source-obj-group*} {*destination-addr destination-wildcard* | **any | host** *dest-addr* | **object-group** *dest-obj-group* | *port-match-criteria* {*destination-addr destination-wildcard* | **any | host** *dest-addr* | **object-group** *dest-obj-group*}} [*port-match-criteria port-number*] [**fragments**] [**ack | established**] [**fin**] [**psh**] [**rst**] [**syn**] [**urg**] [**match-all** *match-value* | **match-any** *match-value*] [**dscp** *dscp-value* | **precedence** *precedence-value*] [**option** *option-value*] [**time-range** *time-range-value*] [**ttl** *match-value ttl-value* [*ttl-value*]] [**tos** *tos-value*]] [**log** [*log-value*] | **log-input** [*log-input-value*]]

no permit {**tcp | udp**}{*source-addr source-wildcard* | **any** | **host** *source-addr* | **object-group** *source-obj-group*} {*destination-addr destination-wild-card* | **any | host** *dest-addr* | **object-group** *dest-obj-group* | *port-match-criteria* {*destination-addr destination-wild-card* | **any | host** *dest-addr* | **object-group** *dest-obj-group*}}

Syntax Description

protocol	Name or number of a protocol; valid values are; valid values are **ahp**, **eigrp**, **esp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **object-group**, **tcp**, **pcp**, **pim**, **udp**, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP), use the keyword **ip**. See the "Usage Guidelines" section for additional qualifiers.
source-addr	(Optional) Number of the network or host from which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.
source-wildcard	(Optional) Wildcard bits to be applied to the source in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.
any	Specifies any source or any destination host as an abbreviation for the *source-addr* or *destination-addr value* and the *source-wildcard* or *destination-wildcard* value of 0.0.0.0 255.255.255.255.
host *address name*	Specifies the source or destination address and name of a single host.
object-group *object-group-name*	Specifies the source or destination name of the object group.
destination-addr	Number of the network or host to which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.

destination-wildcard	Wildcard bits to be applied to the destination in a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.
object-group *dest-addr-group-name*	Specifies the destination address group name.
dscp *dscp-value*	(Optional) Matches the packets with the given Differentiated Services Code Point (DSCP) value; see the "Usage Guidelines" section for valid values.
precedence *precedence-value*	(Optional) Specifies the precedence filtering level for packets; valid values are a number from 0 to 7 or by a name. See the "Usage Guidelines" section for a list of valid names.
fragments *fragment-value*	(Optional) Applies the access list entry to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the "Access List or OGACL Processing of Fragments" and "Fragments and Policy Routing" sections in the "Usage Guidelines" section.
option *option-value*	(Optional) Matches the packets with the given IP options value number; see the "Usage Guidelines" section for valid values.
reflect *access-list-name*	(Optional) Create reflexive access list entry.
time-range *time-range-value*	(Optional) Specifies a time-range entry name.
ttl *match-value ttl-value*	(Optional) Specifies the match packets with given TTL value; see the "Usage Guidelines" section for valid values.
tos *tos-value*	(Optional) Specifies the service filtering level for packets; valid values are a number from 0 to 15 or by a name as listed in the "Usage Guidelines" section of the **access-list** (IP extended) command.
timeout *max-time*	Specifies the maximum time for a reflexive ACL to live; the valid values are from 1 to 2147483 seconds.

log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message for a standard list includes the access list number, whether the packet was permitted or denied, the source address, and the number of packets. The message for an extended list includes the access list number; whether the packet was permitted or denied; the protocol; whether the protocol was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and port numbers and the user-defined cookie or router-generated hash value. For both standard and extended lists, the message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from reloading because of too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list. After you specify the **log** keyword (and the associated *word* argument), you cannot specify any other keywords or settings for this command.
log-value	(Optional) User-defined cookie appended to the log message. The cookie: • cannot be more than characters • cannot start with hexadecimal notation (such as 0x) • cannot be the same as, or a subset of, the following keywords: **reflect**, **fragment**, **time-range** • must contain alphanumeric characters only The user-defined cookie is appended to the access control entry (ACE) syslog entry and uniquely identifies the ACE, within the access control list, that generated the syslog entry.
log-input *log-input-value*	(Optional) Matches the log against this entry, including the input interface. After you specify the **log-input** keyword (and the associated *log-input-value* argument), you cannot specify any other keywords or settings for this command.
tcp	Specifies the TCP protocol.
udp	Specifies the UDP protocol.
object-group *source-obj-group*	Specifies the source address group name.
port-match-criteria port-number	Matches only packets on a given port number; see the "Usage Guidelines" section for valid values.

Command Default There are no specific conditions under which a packet passes the access list.

Command Modes

Standard access-list configuration (config-std-nacl)
Extended access-list configuration (config-ext-nacl)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.4(22)T	The *word* argument was added to the **log** and **log-input** keywords.

Usage Guidelines

Use this command following the **ip access-list** command to define the conditions under which a packet passes the access list.

In Cisco IOS 15.0(1)M and later Releases, to remove the log entry from the **permit ip any any log** command, use the **permit ip any any** command.

In releases earlier than Cisco IOS Release15.0(1)M, to remove the **log** option from the **permit ip any any log** command, use the **no permit ip any any log** and the **permit ip any any** commands.

In Cisco IOS 15.0(1)M and later releases, to remove the log entry and the user-defined cookie, use the **permit ip any any** [*log-value*] command.

In releases earlier than Cisco IOS Release 15.0(1)M, to remove the log entry and user-defined cookies, use the **no permit ip any any log** [*log-value*] and **permit ip any any** commands.

Access List or OGACL Processing of Fragments

The behavior of access-list entries regarding the use or lack of the **fragments** keyword are summarized in Table 50:

Table 50 Access list or OGACL Processing of Fragments

If the Access-List Entry Has...	Then...
...no **fragments** keyword (the default behavior), and assuming all of the access-list entry information matches,	For an access-list entry containing only Layer 3 information: • The entry is applied to nonfragmented packets, initial fragments, and noninitial fragments. For an access list entry containing Layer 3 and Layer 4 information: • The entry is applied to nonfragmented packets and initial fragments: – If the entry is a **permit** statement, the packet or fragment is permitted. – If the entry is a **deny** statement, the packet or fragment is denied. • The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access-list entry can be applied. If the Layer 3 portion of the access-list entry matches, and – If the entry is a **permit** statement, the noninitial fragment is permitted. – If the entry is a **deny** statement, the next access-list entry is processed. **Note** The **deny** statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.
...the **fragments** keyword, and assuming all of the access-list entry information matches,	**Note** The access-list entry is applied only to noninitial fragments. The **fragments** keyword cannot be configured for an access-list entry that contains any Layer 4 information.

Ensure that you do not add the **fragments** keyword to every access list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments** keyword, the packet is compared to the next access list entry, and so on, until it is either permitted or denied by an access list entry that does not contain the **fragments** keyword. Therefore, you may need two access list entries for every **deny** entry. The first **deny** entry of the pair will not include the **fragments** keyword, and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases where there are multiple

deny access list entries for the same host but with different Layer 4 ports, a single **deny** access-list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets and each counts individually as a packet in access list accounting and access list violation counts.

Note The **fragments** keyword cannot solve all cases involving access lists and IP fragments.

Fragments and Policy Routing

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip address** command and the access list had entries that match on Layer 4 through 7 information. It is possible that noninitial fragments pass the access list and are policy routed, even if the first fragment was not policy routed or the reverse.

By using the **fragments** keyword in access list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made and it is more likely policy routing will occur as intended.

The *source-addr* and *destination-addr* arguments allow you to create an object group based on a source or destination group. The following keywords and arguments are available:

- **dscp** *dscp-value*—(Optional) Matches the packets with the given DSCP value; the valid values are as follows:
  - **0** to **63**—Differentiated services codepoint value
  - **af11**—Matches the packets with AF11 dscp (001010)
  - **af12**—Matches the packets with AF12 dscp (001100)
  - **af13**—Matches the packets with AF13 dscp (001110)
  - **af21**—Matches the packets with AF21 dscp (010010)
  - **af22**—Matches the packets with AF22 dscp (010100)
  - **af23**—Matches the packets with AF23 dscp (010110)
  - **af31**—Matches the packets with AF31 dscp (011010)
  - **af32**—Matches the packets with AF32 dscp (011100)
  - **af33**—Matches the packets with AF33 dscp (011110)
  - **af41**—Matches the packets with AF41 dscp (100010)
  - **af42**—Matches the packets with AF42 dscp (100100)
  - **af43**—Matches the packets with AF43 dscp (100110)
  - **cs1**—Matches the packets with CS1 (precedence 1) dscp (001000)
  - **cs2**—Matches the packets with CS2 (precedence 2) dscp (010000)
  - **cs3**—Matches the packets with CS3 (precedence 3) dscp (011000)
  - **cs4**—Matches the packets with CS4 (precedence 4) dscp (100000)
  - **cs5**—Matches the packets with CS5 (precedence 5) dscp (101000)
  - **cs6**—Matches the packets with CS6 (precedence 6) dscp (110000)
  - **cs7**—Matches the packets with CS7 (precedence 7) dscp (111000)
  - **default**—Matches the packets with default dscp (000000)

  - **ef**—Matches the packets with EF dscp (101110)
- **fragments**—(Optional) Checks for noninitial fragments. See Table 50.
- **log**—(Optional) Logs the matches against this entry.
- **log-input**—(Optional) Logs the matches against this entry, including the input interface.
- **option** *option-value*—(Optional) Matches the packets with given IP Options value. The valid values are as follows:
  - **0** to **255**—IP Options value.
  - **add-ext**—Matches the packets with Address Extension Option (147).
  - **any-options**—Matches the packets with ANY Option.
  - **com-security**—Matches the packets with Commercial Security Option (134).
  - **dps**—Matches the packets with Dynamic Packet State Option (151).
  - **encode**—Matches the packets with Encode Option (15).
  - **eool**—Matches the packets with End of Options (0).
  - **ext-ip**—Matches the packets with Extended IP Option (145).
  - **ext-security**—Matches the packets with Extended Security Option (133).
  - **finn**—Matches the packets with Experimental Flow Control Option (205).
  - **imitd**—Matches the packets with IMI Traffic Desriptor Option (144).
  - **lsr**—Matches the packets with Loose Source Route Option (131).
  - **match-all**—Matches the packets if all specified flags are present.
  - **match-any**—Matches the packets if any specified flag is present.
  - **mtup**—Matches the packets with MTU Probe Option (11).
  - **mtur**—Matches the packets with MTU Reply Option (12).
  - **no-op**—Matches the packets with No Operation Option (1).
  - **psh**—Match the packets on the PSH bit.
  - **nsapa**—Matches the packets with NSAP Addresses Option (150).
  - **reflect**—Creates reflexive access list entry.
  - **record-route**—Matches the packets with Record Route Option (7).
  - **rst**—Matches the packets on the RST bit.
  - **router-alert**—Matches the packets with Router Alert Option (148).
  - **sdb**—Matches the packets with Selective Directed Broadcast Option (149).
  - **security**—Matches the packets with Basic Security Option (130).
  - **ssr**—Matches the packets with Strict Source Routing Option (137).
  - **stream-id**—Matches the packets with Stream ID Option (136).
  - **syn**—Matches the packets on the SYN bit.
  - **timestamp**—Matches the packets with Time Stamp Option (68).
  - **traceroute**—Matches the packets with Trace Route Option (82).
  - **ump**—Matches the packets with Upstream Multicast Packet Option (152).
  - **visa**—Matches the packets with Experimental Access Control Option (142).

  - **zsu**—Matches the packets with Experimental Measurement Option (10).
- **precedence** *precedence-value*—(Optional) Matches the packets with given precedence value; the valid values are as follows:
  - **0** to **7**—Precedence value.
  - **critical**—Matches the packets with critical precedence (5).
  - **flash**—Matches the packets with flash precedence (3).
  - **flash-override**—Matches the packets with flash override precedence (4).
  - **immediate**—Matches the packets with immediate precedence (2).
  - **internet**—Matches the packets with internetwork control precedence (6).
  - **network**—Matches the packets with network control precedence (7).
  - **priority**—Matches the packets with priority precedence (1).
  - **routine**—Matches the packets with routine precedence (0).
- **reflect acl-name**—(Optional) Creates reflexive access list entry.
- **ttl** *match-value ttl-value*—(Optional) Specifies the match packets with given TTL value; the valid values are as follows:
  - **eq**—Matches packets on a given TTL number.
  - **gt**—Matches packets with a greater TTL number.
  - **lt**—Matches packets with a lower TTL number.
  - **neq**—Matches packets not on a given TTL number.
  - **range**—Matches packets in the range of TTLs.
- **time-range** *time-range-value*—(Optional) Specifies a time-range entry name.
- **tos**—(Optional) Matches the packets with given ToS value; the valid values are as follows:
  - **0** to **15**—Type of service value.
  - **max-reliability**—Matches the packets with the maximum reliable ToS (2).
  - **max-throughput**—Matches the packets with the maximum throughput ToS (4).
  - **min-delay**—Matches the packets with the minimum delay ToS (8).
  - **min-monetary-cost**—Matches the packets with the minimum monetary cost ToS (1).
  - **normal**—Matches the packets with the normal ToS (0).
- **timeout** *max-time*—(Optional) Specifies the maximum time for a reflexive ACL to live; the valid values are from 1 to 2147483 seconds.

Examples

The following example shows how to create an access list that permits packets from the users in my_network_object_group if the protocol ports match the ports specified in my_network_object_group:

```
Router> enable
Router# configure terminal
Router(config)# ip access-list extended my_ogacl_policy
Router(config-ext-nacl)# permit tcp object-group my_network_object_group portgroup
my_service_object_group any
```

The following example shows how to create an access list that permits packets from the users in my_network_object_group if the protocol ports match the ports specified in my_network_object_group. In addition, logging is enabled for the access list, and all syslog entries for this ACE include the word MyServiceCookieValue:

```
Router> enable
Router# configure terminal
Router(config)# ip access-list extended my_ogacl_policy
Router(config-ext-nacl)# permit tcp object-group my_network_object_group portgroup
my_service_object_group any log MyServiceCookieValue
```

Related Commands

Command	Description
deny	Sets conditions in a named IP access list or OGACL that will deny packets.
ip access-group	Applies an ACL or OGACL to an interface or a service policy map.
ip access-list	Defines an IP access list or OGACL by name or number.
ip access-list logging hash-generation	Enables hash value generation for ACE syslog entries.
object-group network	Defines network object groups for use in OGACLs.
object-group service	Defines service object groups for use in OGACLs.
show ip access-list	Displays the contents of IP access lists or OGACLs.
show object-group	Displays information about object groups that are configured.

permit (Catalyst 6500 series switches)

To set conditions for a named IP access list, use the **permit** command in access-list configuration mode. To remove a condition from an access list, use the **no** form of this command.

permit *protocol* {{*source-addr source-wildcard*} | **addrgroup** *object-group-name* | **any** | **host** {*address* | *name*}} {*destination-addr destination-wildcard*} | **addrgroup** *object-group-name* | **any** | **host** {*address* | *name*}}

permit {**tcp** | **udp**} {{*source-addr source-wildcard*} | **addrgroup** *source-addr-group-name* | **any** | **host** {*address* | *name*} {*destination-addr destination-wildcard* | **any** | **eq** *port* | **gt** *port* | **host** {*address* | *name*} | **lt** *port* | **neq** *port* | **portgroup** *srcport-groupname*} {**addrgroup** *dest-addr-groupname* | *destination* | *destination-addr destination-wildcard* | **any** | **eq** *port* | **gt** *port* | **host** {*address* | *name*} | **lt** *port* | **neq** *port* | **portgroup** *destport-groupname*} [**dscp** *type*] [**fragments**] [**option** *option*] [**precedence** *precedence*] [**time-range** *time-range-name*] [**tos** *tos*]] [**log** [*word*] | **log-input** [*word*]]}

no permit *protocol* {{*source-addr source-wildcard*} | **addrgroup** *object-group-name* | **any** | **host** {*address* | *name*}} {*destination-addr destination-wildcard*} | **addrgroup** *object-group-name* | **any** | **host** {*address* | *name*}}

no permit {**tcp** | **udp**} {{*source-addr source-wildcard*} | **addrgroup** *source-addr-group-name* | **any** | **host** {*address* | *name*} {*destination-addr destination-wildcard* | **any** | **eq** *port* | **gt** *port* | **host** {*address* | *name*} | **lt** *port* | **neq** *port* | **portgroup** *srcport-groupname*} {**addrgroup** *dest-addr-groupname* | *destination* | *destination-addr destination-wildcard* | **any** | **eq** *port* | **gt** *port* | **host** {*address* | *name*} | **lt** *port* | **neq** *port* | **portgroup** *destport-groupname*} [**dscp** *type*] [**fragments**] [**option** *option*] [**precedence** *precedence*] [**time-range** *time-range-name*] [**tos** *tos*]] [**log** [*word*] | **log-input** [*word*]]}

Syntax Description

protocol	Name or number of a protocol; valid values are **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, or **udp**, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP), use the keyword **ip**. See the "Usage Guidelines" section for additional qualifiers.
source-addr	Number of the network or host from which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.
source-wildcard	Wildcard bits to be applied to source in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.
addrgroup *object-group-name*	Specifies the source or destination name of the object group.
any	Specifies any source or any destination host as an abbreviation for the *source-addr* or *destination-addr value* and the *source-wildcard* or *destination-wildcard* value of 0.0.0.0 255.255.255.255.
host *address*	Specifies the source or destination address of a single host.
host *name*	Specifies the source or destination name of a single host.
tcp	Specifies the TCP protocol.
udp	Specifies the UDP protocol.

addrgroup *source-addr-group-name*	Specifies the source address group name.
destination-addr	Number of the network or host to which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.
destination-wildcard	Wildcard bits to be applied to the destination in a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.
eq *port*	Matches only packets on a given port number; see the "Usage Guidelines" section for valid values.
gt *port*	Matches only the packets with a greater port number; see the "Usage Guidelines" section for valid values.
lt *port*	Matches only the packets with a lower port number; see the "Usage Guidelines" section for valid values.
neq *port*	Matches only the packets that are not on a given port number; see the "Usage Guidelines" section for valid values.
portgroup *srcport-group-name*	Specifies the source port object group name.
addrgroup *dest-addr-group-name*	Specifies the destination address group name.
portgroup *destport-group-name*	Specifies the destination port object group name.
dscp *type*	(Optional) Matches the packets with the given Differentiated Services Code Point (DSCP) value; see the "Usage Guidelines" section for valid values.
fragments	(Optional) Applies the access list entry to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the "Access List Processing of Fragments" and "Fragments and Policy Routing" sections in the "Usage Guidelines" section.
option *option*	(Optional) Matches the packets with the given IP options value number; see the "Usage Guidelines" section for valid values.
precedence *precedence*	(Optional) Specifies the precedence filtering level for packets; valid values are a number from 0 to 7 or by a name. See the "Usage Guidelines" section for a list of valid names.
time-range *time-range-name*	(Optional) Specifies a time-range entry name.
tos *tos*	(Optional) Specifies the service filtering level for packets; valid values are a number from 0 to 15 or by a name as listed in the "Usage Guidelines" section of the **access-list** (IP extended) command.
option option	(Optional) Matches packets with the IP options value; see the "Usage Guidelines" section for the valid values.
fragments	(Optional) Applies the access list entry to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the "Access List Processing of Fragments" and "Fragments and Policy Routing" sections in the "Usage Guidelines" section.

log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message for a standard list includes the access list number, whether the packet was permitted or denied, the source address, and the number of packets, and if appropriate, the user-defined cookie or router-generated hash value. The message for an extended list includes the access list number; whether the packet was permitted or denied; the protocol; whether the protocol was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers, and if appropriate, the user-defined cookie or router-generated hash value. For both standard and extended lists, the message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from reloading due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list. After you specify the **log** keyword (and the associated *word* argument), you cannot specify any other keywords or settings for this command.
word	(Optional) User-defined cookie appended to the log message. The cookie: • cannot be more than characters • cannot start with hexadecimal notation (such as 0x) • cannot be the same as, or a subset of, the following keywords: **reflect**, **fragment**, **time-range** • must contain alphanumeric characters only The user-defined cookie is appended to the access control entry (ACE) syslog entry and uniquely identifies the ACE, within the access control list, that generated the syslog entry.
log-input	(Optional) Matches the log against this entry, including the input interface. After you specify the **log-input** keyword (and the associated *word* argument), you cannot specify any other keywords or settings for this command.

Command Default There are no specific conditions under which a packet passes the named access list.

Command Modes Access-list configuration (config-ext-nacl)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.4(22)T	The *word* argument was added to the **log** and **log-input** keywords.

Usage Guidelines

Use this command following the **ip access-list** command to define the conditions under which a packet passes the access list.

The **portgroup** keyword appears only when you configure an extended access list.

Access List Processing of Fragments

The behavior of access-list entries regarding the use or lack of the **fragments** keyword are summarized in Table 51:

Table 51 Access list Processing of Fragments

If the Access-List Entry Has...	Then...
...no **fragments** keyword (the default behavior), and assuming all of the access-list entry information matches,	For an access-list entry containing only Layer 3 information: • The entry is applied to nonfragmented packets, initial fragments, and noninitial fragments. For an access list entry containing Layer 3 and Layer 4 information: • The entry is applied to nonfragmented packets and initial fragments: – If the entry is a **permit** statement, the packet or fragment is permitted. – If the entry is a **deny** statement, the packet or fragment is denied. • The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access-list entry can be applied. If the Layer 3 portion of the access-list entry matches, and – If the entry is a **permit** statement, the noninitial fragment is permitted. – If the entry is a **deny** statement, the next access-list entry is processed. **Note** The **deny** statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.
...the **fragments** keyword, and assuming all of the access-list entry information matches,	**Note** The access-list entry is applied only to noninitial fragments.The **fragments** keyword cannot be configured for an access-list entry that contains any Layer 4 information.

Be aware that you should not simply add the **fragments** keyword to every access list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments** keyword, the packet is compared to the next access list entry, and so on, until it is either permitted or denied by an access list entry that does not contain the **fragments** keyword. Therefore, you may need two access list entries for every **deny** entry. The first **deny** entry of the pair will not include the **fragments** keyword, and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases where there are multiple **deny** access list entries for the same host but with different Layer 4 ports, a single **deny** access-list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets and each counts individually as a packet in access list accounting and access list violation counts.

Note The **fragments** keyword cannot solve all cases involving access lists and IP fragments.

Fragments and Policy Routing

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip address**s command and the access list had entries that match on Layer 4 through 7 information. It is possible that noninitial fragments pass the access list and are policy routed, even if the first fragment was not policy routed or the reverse.

By using the **fragments** keyword in access list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made and it is more likely policy routing will occur as intended.

The **portgroup** *srcport-groupname or* **portgroup** *destport-groupname* keywords and arguments allow you to create an object group based on a source or destination group. The following keywords and arguments are available:

- **dscp** *value*—(Optional) Matches the packets with the given DSCP value; the valid values are as follows:
  - **0** to **63**—Differentiated services codepoint value
  - **af11**—Matches the packets with AF11 dscp (001010)
  - **af12**—Matches the packets with AF12 dscp (001100)
  - **af13**—Matches the packets with AF13 dscp (001110)
  - **af21**—Matches the packets with AF21 dscp (010010)
  - **af22**—Matches the packets with AF22 dscp (010100)
  - **af23**—Matches the packets with AF23 dscp (010110)
  - **af31**—Matches the packets with AF31 dscp (011010)
  - **af32**—Matches the packets with AF32 dscp (011100)
  - **af33**—Matches the packets with AF33 dscp (011110)
  - **af41**—Matches the packets with AF41 dscp (100010)
  - **af42**—Matches the packets with AF42 dscp (100100)
  - **af43**—Matches the packets with AF43 dscp (100110)
  - **cs1**—Matches the packets with CS1(precedence 1) dscp (001000)

  - **cs2**—Matches the packets with CS2(precedence 2) dscp (010000)
  - **cs3**—Matches the packets with CS3(precedence 3) dscp (011000)
  - **cs4**—Matches the packets with CS4(precedence 4) dscp (100000)
  - **cs5**—Matches the packets with CS5(precedence 5) dscp (101000)
  - **cs6**—Matches the packets with CS6(precedence 6) dscp (110000)
  - **cs7**—Matches the packets with CS7(precedence 7) dscp (111000)
  - **default**—Matches the packets with default dscp (000000)
  - **ef**—Matches the packets with EF dscp (101110)
- **fragments**—(Optional) Checks for noninitial fragments. See the table "Access List Processing of Fragments."
- **log**—(Optional) Logs the matches against this entry.
- **log-input**—(Optional) Logs the matches against this entry, including the input interface; the valid values are as follows:
- **option** *option*—(Optional) Matches the packets with given IP Options value. The valid values are as follows:
  - **0** to **255**—IP Options value.
  - **add-ext**—Matches the packets with Address Extension Option (147).
  - **any-options**—Matches the packets with ANY Option.
  - **com-security**—Matches the packets with Commercial Security Option (134).
  - **dps**—Matches the packets with Dynamic Packet State Option (151).
  - **encode**—Matches the packets with Encode Option (15).
  - **eool**—Matches the packets with End of Options (0).
  - **ext-ip**—Matches the packets with Extended IP Option (145).
  - **ext-security**—Matches the packets with Extended Security Option (133).
  - **finn**—Matches the packets with Experimental Flow Control Option (205).
  - **imitd**—Matches the packets with IMI Traffic Desriptor Option (144).
  - **lsr**—Matches the packets with Loose Source Route Option (131).
  - **match-all**—Matches the packets if all specified flags are present.
  - **match-any**—Matches the packets if any specified flag is present.
  - **mtup**—Matches the packets with MTU Probe Option (11).
  - **mtur**—Matches the packets with MTU Reply Option (12).
  - **no-op**—Matches the packets with No Operation Option (1).
  - **psh**—Match the packets on the PSH bit.
  - **nsapa**—Matches the packets with NSAP Addresses Option (150).
  - **reflect**—Creates reflexive access list entry.
  - **record-route**—Matches the packets with Record Route Option (7).
  - **rst**—Matches the packets on the RST bit.
  - **router-alert**—Matches the packets with Router Alert Option (148).

  - **sdb**—Matches the packets with Selective Directed Broadcast Option (149).
  - **security**—Matches the packets with Basic Security Option (130).
  - **ssr**—Matches the packets with Strict Source Routing Option (137).
  - **stream-id**—Matches the packets with Stream ID Option (136).
  - **syn**—Matches the packets on the SYN bit.
  - **timestamp**—Matches the packets with Time Stamp Option (68).
  - **traceroute**—Matches the packets with Trace Route Option (82).
  - **ump**—Matches the packets with Upstream Multicast Packet Option (152).
  - **visa**—Matches the packets with Experimental Access Control Option (142).
  - **zsu**—Matches the packets with Experimental Measurement Option (10).
- **precedence** *value*—(Optional) Matches the packets with given precedence value; the valid values are as follows:
  - **0** to **7**—Precedence value.
  - **critical**—Matches the packets with critical precedence (5).
  - **flash**—Matches the packets with flash precedence (3).
  - **flash-override**—Matches the packets with flash override precedence (4).
  - **immediate**—Matches the packets with immediate precedence (2).
  - **internet**—Matches the packets with internetwork control precedence (6).
  - **network**—Matches the packets with network control precedence (7).
  - **priority**—Matches the packets with priority precedence (1).
  - **routine**—Matches the packets with routine precedence (0).
- **reflect acl-name** [**timeout** *time*]—(Optional) Creates reflexive access list entry. The **timeout** *time* keyword and argument specify the maximum time for a reflexive ACL to live; the valid values are from 1 to 2147483 seconds.
- **time-range** *name*—(Optional) Specifies a time-range entry name.
- **tos**—(Optional) Matches the packets with given ToS value; the valid values are as follows:
  - **0** to**15**—Type of service value.
  - **max-reliability**—Matches the packets with the maximum reliable ToS (2).
  - **max-throughput**—Matches the packets with the maximum throughput ToS (4).
  - **min-delay**—Matches the packets with the minimum delay ToS (8).
  - **min-monetary-cost**—Matches the packets with the minimum monetary cost ToS (1).
  - **normal**—Matches the packets with the normal ToS (0).

Examples

The following example shows how to create an access list that permits packets from the users in myAG if the protocol ports match the ports specified in myPG:

```
Router(config)# ip access-list extended my-pbacl-policy
Router(config-ext-nacl)# permit tcp addrgroup myAG portgroup myPG any
```

The following example shows how to create an access list that permits packets from the users in myAG if the protocol ports match the ports specified in myPG. The access list is log enabled, and the cookie value is set to myCookie:

```
Router(config)# ip access-list extended my-pbacl-policy
Router(config-ext-nacl)# permit tcp addrgroup myAG portgroup myPG any log myCookie
```

Related Commands

Command	Description
deny (Catalyst 6500 series switches)	Sets conditions for a named IP access list.
ip access-group	Controls access to an interface.
ip access-list	Defines an IP access list by name.
ip access-list logging hash-generation	Enables hash value generation for ACE syslog entries.
show ip access-lists	Displays the contents of all current IP access lists.

permit (IP)

To set conditions to allow a packet to pass a named IP access list, use the **permit** command in access list configuration mode. To remove a permit condition from an access list, use the **no** form of this command.

[*sequence-number*] **permit** *source* [*source-wildcard*]

[*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard* [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**time-range** *time-range-name*] [**fragments**] [**log** [*user-defined-cookie*]]

no *sequence-number*

no permit *source* [*source-wildcard*]

no permit *protocol source source-wildcard destination destination-wildcard* [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**time-range** *time-range-name*] [**fragments**] [**log** [*user-defined-cookie*]]

Internet Control Message Protocol (ICMP)

[*sequence-number*] **permit icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* [*icmp-code*] | *icmp-message*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**time-range** *time-range-name*] [**fragments**] [**log** [*user-defined-cookie*]]

Internet Group Management Protocol (IGMP)

[*sequence-number*] **permit igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**time-range** *time-range-name*] [**fragments**] [**log** [*user-defined-cookie*]]

Transmission Control Protocol (TCP)

[*sequence-number*] **permit tcp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established** | {**match-any** | **match-all**} {**+** | **-**} *flag-name*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**time-range** *time-range-name*] [**fragments**] [**log** [*user-defined-cookie*]]

User Datagram Protocol (UDP)

[*sequence-number*] **permit udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**time-range** *time-range-name*] [**fragments**] [**log** [*user-defined-cookie*]]

Syntax Description

sequence-number	(Optional) Sequence number assigned to the permit statement. The sequence number causes the system to insert the statement in that numbered position in the access list.
source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
source-wildcard	(Optional) Wildcard bits to be applied to the source. There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part dotted-decimal format. Place 1s in the bit positions that you want to ignore. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
protocol	Name or number of an Internet protocol. The *protocol* argument can be one of the keywords **eigrp**, **gre**, **icmp**, **igmp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, or **udp**, or an integer in the range from 0 to 255 representing an Internet protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the **ip** keyword. **Note** When the **icmp**, **igmp**, **tcp,** and **udp** keywords are entered, they must be followed with the specific command syntax that is shown for the ICMP, IGMP, TCP, and UDP forms of the **permit** command. **Note** To configure a packet filter to allow BGP traffic, use protocol **tcp** and specify the port number as 179 or **bgp**.
destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part dotted-decimal format. Place 1s in the bit positions that you want to ignore. • Use the **any** keyword as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.

option *option-name*	(Optional) Packets can be filtered by IP Options, as specified by a number from 0 to 255, or by the corresponding IP Option name, as listed in Table 52 in the "Usage Guidelines" section.
precedence *precedence*	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7 or by a name.
tos *tos*	(Optional) Packets can be filtered by type of service (ToS) level, as specified by a number from 0 to 15, or by a name as listed in the "Usage Guidelines" section of the **access-list** (IP extended) command.
ttl *operator value*	(Optional) Compares the TTL value in the packet to the TTL value specified in this **permit** statement. • The *operator* can be **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), or **range** (inclusive range). • The *value* can range from 0 to 255. • If the operator is **range**, specify two values separated by a space. • For Release 12.0S, if the operator is **eq** or **neq**, only one TTL value can be specified. • For all other releases, if the operator is **eq** or **neq**, as many as 10 TTL values can be specified, separated by a space.
time-range *time-range-name*	(Optional) Name of the time range that applies to this **permit** statement. The name of the time range and its restrictions are specified by the **time-range** and **absolute** or **periodic** commands, respectively.
fragments	(Optional) The access list entry applies to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the "Access List Processing of Fragments" and "Fragments and Policy Routing" sections in the "Usage Guidelines" section.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) After you specify the **log** keyword (and the associated *word* argument), you cannot specify any other keywords or settings for this command.
user-defined-cookie	(Optional) User-defined cookie appended to the log message. The cookie: • Cannot be more than 64 characters. • Cannot start with hexadecimal notation (such as 0x). • Cannot be the same as, or a subset of, the following keywords: **fragment, reflect**, **time-range**. • Must contain alphanumeric characters only. The user-defined cookie is appended to the Allegro Crypto Engine (ACE) syslog entry and uniquely identifies the ACE, within the access control list, that generated the syslog entry.
icmp	Permits only ICMP packets. When you enter the **icmp** keyword, you must use the specific command syntax shown for the ICMP form of the **permit** command.
icmp-type	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.

icmp-code	(Optional) ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
icmp-message	(Optional) ICMP packets can be filtered by an ICMP message type name or an ICMP message type and code name. The possible names are listed in the "Usage Guidelines" section of the **access-list** (IP extended) command.
igmp	Permits only IGMP packets. When you enter the **igmp** keyword, you must use the specific command syntax shown for the IGMP form of the **permit** command.
igmp-type	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the "Usage Guidelines" section of the **access-list** (IP extended) command.
tcp	Permits only TCP packets. When you enter the **tcp** keyword, you must use the specific command syntax shown for the TCP form of the **permit** command.
operator	(Optional) Compares source or destination ports. Operators are **eq** (equal) , **gt** (greater than),**lt** (less than), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source* and *source-wildcard* arguments, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard* arguments, it must match the destination port. The **range** operator requires two port numbers. Up to ten port numbers can be entered for the **eq** (equal) and **neq** (not equal) operators. All other operators require one port number.
port	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the "Usage Guidelines" section of the **access-list** (IP extended) command. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bit set. The nonmatching case is that of the initial TCP datagram to form a connection.
{**match-any** | **match-all**}	(Optional) For the TCP protocol only: A match occurs if the TCP datagram has certain TCP flags set or not set. You use the **match-any** keyword to allow a match to occur if any of the specified TCP flags are present, or you can use the **match-all** keyword to allow a match to occur only if all of the specified TCP flags are present. You must follow the **match-any** and **match-all** keywords with the **+** or **-** keyword and the *flag-name* argument to match on one or more TCP flags.

{**+** | **-**} *flag-name*	(Optional) For the TCP protocol only: The **+** keyword matches IP packets if their TCP headers contain the TCP flags that are specified by the *flag-name* argument. The **-** keyword matches IP packets that do not contain the TCP flags specified by the *flag-name* argument. You must follow the **+** and **-** keywords with the *flag-name* argument. TCP flag names can be used only when filtering TCP. Flag names for the TCP flags are as follows: **ack**, **fin**, **psh**, **rst**, **syn**, and **urg**.
udp	Permits only UDP packets. When you enter the **udp** keyword, you must use the specific command syntax shown for the UDP form of the **permit** command.

Command Default

There are no specific conditions under which a packet passes the named access list.

Command Modes

Access list configuration (config-ext-nacl)

Command History

Release	Modification
11.2	This command was introduced.
12.0(1)T	The **time-range** *time-range-name* keyword and argument were added.
12.0(11)	The **fragments** keyword was added.
12.2(13)T	The **igrp** keyword was removed because the IGRP protocol was no longer available in Cisco IOS software.
12.2(14)S	The *sequence-number* argument was added.
12.2(15)T	The *sequence-number* argument was added.
12.3(4)T	The **option** *option-name* keyword and argument were added. The **match-any**, **match-all, +**, and **-** keywords and the *flag-name* argument were added.
12.3(7)T	Command functionality was modified to allow up to ten port numbers to be added after the **eq** and **neq** operators so that an access list entry can be created with noncontiguous ports.
12.4	The **drip** keyword was added to specify the TCP port number used for Optimized Edge Routing (OER) communication.
12.4(2)T	The **ttl** *operator value* keyword and arguments were added.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(22)T	The *word* argument was added to the **log** keyword.
Cisco IOS XE Release 3.2	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

Use this command following the **ip access-list** command to define the conditions under which a packet passes the named access list.

The **time-range** keyword allows you to identify a time range by name. The **time-range**, **absolute**, and **periodic** commands specify when this **permit** statement is in effect.

log Keyword

A log message includes the access list number or access list name, and whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and port numbers, and the user-defined cookie or router-generated hash value. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval.

Use the **ip access-list log-update** command to generate logging messages when the number of matches reaches a configurable threshold (rather than waiting for a 5-minute-interval). See the **ip access-list log-update** command for more information.

The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from reloading because of too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.

If you enable Cisco Express Forwarding and then create an access list that uses the **log** keyword, the packets that match the access list are not Cisco Express Forwarding switched. They are fast-switched. Logging disables Cisco Express Forwarding .

Access List Filtering of IP Options

Access control lists can be used to filter packets with IP Options to prevent routers from being saturated with spurious packets containing IP Options. To see a complete table of all IP Options, including ones currently not in use, refer to the latest Internet Assigned Numbers Authority (IANA) information that is available from its URL: www.iana.org.

Cisco IOS software allows you to filter packets according to whether they contain one or more of the legitimate IP Options by entering either the IP Option value or the corresponding name for the *option-name* argument as shown in Table 52.

Table 52 IP Option Values and Names

IP Option Value or Name	Description
0 to 255	IP Options values.
add-ext	Match packets with Address Extension Option (147).
any-options	Match packets with any IP Option.
com-security	Match packets with Commercial Security Option (134).
dps	Match packets with Dynamic Packet State Option (151).
encode	Match packets with Encode Option (15).
eool	Match packets with End of Options (0).
ext-ip	Match packets with Extended IP Options (145).
ext-security	Match packets with Extended Security Option (133).
finn	Match packets with Experimental Flow Control Option (205).
imitd	Match packets with IMI Traffic Descriptor Option (144).

Table 52 IP Option Values and Names (continued)

IP Option Value or Name	Description
lsr	Match packets with Loose Source Route Option (131).
mtup	Match packets with MTU Probe Option (11).
mtur	Match packets with MTU Reply Option (12).
no-op	Match packets with No Operation Option (1).
nsapa	Match packets with NSAP Addresses Option (150).
psh	Match the packets on the PSH bit.
record-route	Match packets with Router Record Route Option (7).
reflect	Create reflexive access list entry.
router-alert	Match packets with Router Alert Option (148).
rst	Matche the packets on the RST bit.
sdb	Match packets with Selective Directed Broadcast Option (149).
security	Match packets with Base Security Option (130).
ssr	Match packets with Strict Source Routing Option (137).
stream-id	Match packets with Stream ID Option (136).
syn	Matches the packets on the SYN bit.
timestamp	Match packets with Time Stamp Option (68).
traceroute	Match packets with Trace Route Option (82).
ump	Match packets with Upstream Multicast Packet Option (152).
visa	Match packets with Experimental Access Control Option (142).
zsu	Match packets with Experimental Measurement Option (10).

Filtering IP Packets Based on TCP Flags

The access list entries that make up an access list can be configured to detect and drop unauthorized TCP packets by allowing only the packets that have very specific groups of TCP flags set or not set. Users can select any desired combination of TCP flags with which to filter TCP packets. Users can configure access list entries in order to allow matching on a flag that is set and on a flag that is not set. Use the **+** and **-** keywords with a flag name to specify that a match is made based on whether a TCP header flag has been set. Use the **match-any** and **match-all** keywords to allow the packet if any or all, respectively, of the flags specified by the **+** or **-** keyword and *flag-name* argument have been set or not set.

Permitting Optimized Edge Routing (OER) Communication

The **drip** keyword was introduced under the **tcp** keyword to support packet filtering in a network where OER is configured. The **drip** keyword specifies port 3949 that OER uses for internal communication. This option allows you to build a packet filter that permits communication between an OER master controller and border routers. The **drip** keyword is entered following the TCP source, destination addresses, and the **eq** operator. See the example in the "Examples" section.

Access List Processing of Fragments

The behavior of access list entries regarding the use or lack of use of the **fragments** keyword can be summarized as follows:

If the Access-List Entry Has ...	Then ...
... no **fragments** keyword (the default behavior), and assuming all of the access list entry information matches,	For an access list entry that contains only Layer 3 information, the entry is applied to nonfragmented packets, initial fragments, and noninitial fragments. For an access list entry that contains Layer 3 and Layer 4 information: • The entry is applied to nonfragmented packets and initial fragments. – If the entry is a **permit** statement, then the packet or fragment is permitted. – If the entry is a **deny** statement, then the packet or fragment is denied. • The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access list entry can be applied. If the Layer 3 portion of the access list entry matches, and – If the entry is a **permit** statement, then the noninitial fragment is permitted. – If the entry is a **deny** statement, then the next access list entry is processed. **Note** The **deny** statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.
... the **fragments** keyword, and assuming all of the access list entry information matches,	The access list entry is applied only to noninitial fragments. The **fragments** keyword cannot be configured for an access list entry that contains any Layer 4 information.

Be aware that you should not add the **fragments** keyword to every access list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments** keyword. The packet is compared to the next access list entry, and so on, until it is either permitted or denied by an access list entry that does not contain the **fragments** keyword. Therefore, you may need two access list entries for every **deny** entry. The first **deny** entry of the pair will not include the **fragments** keyword and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases in which there are multiple **deny** access list entries for the same host but with different Layer 4 ports, a single **deny** access list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets, and each counts individually as a packet in access list accounting and access list violation counts.

Note The **fragments** keyword cannot solve all cases that involve access lists and IP fragments.

Fragments and Policy Routing

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip address** command and the access list has entries that match on Layer 4 through 7 information. It is possible that noninitial fragments pass the access list and are policy-routed, even if the first fragment is not policy-routed.

If you specify the **fragments** keyword in access list entries, a better match between the action taken for initial and noninitial fragments can be made, and it is more likely that policy routing will occur as intended.

Creating an Access List Entry with Noncontiguous Ports

For Cisco IOS Release 12.3(7)T and later releases, you can specify noncontiguous ports on the same access control entry, which greatly reduces the number of access list entries required for the same source address, destination address, and protocol. If you maintain large numbers of access list entries, we recommend that you consolidate them when possible by using noncontiguous ports. You can specify up to ten port numbers following the **eq** and **neq** operators.

Examples

The following example shows how to set conditions for a standard access list named Internetfilter:

```
ip access-list standard Internetfilter
 deny 192.168.34.0  0.0.0.255
 permit 172.16.0.0  0.0.255.255
 permit 10.0.0.0  0.255.255.255
! (Note: all other access implicitly denied).
```

The following example shows how to permit Telnet traffic on Mondays, Tuesdays, and Fridays from 9:00 a.m. to 5:00 p.m.:

```
time-range testing
 periodic Monday Tuesday Friday 9:00 to 17:00
!
ip access-list extended legal
 permit tcp any any eq telnet time-range testing
!
interface ethernet0
 ip access-group legal in
```

The following example shows how to set a permit condition for an extended access list named filter2. The access list entry specifies that a packet may pass the named access list only if it contains the NSAP Addresses IP Option, which is represented by the IP Option value nsapa.

```
ip access-list extended filter2
 permit ip any any option nsapa
```

The following example shows how to set a permit condition for an extended access list named kmdfilter1. The access list entry specifies that a packet can pass the named access list only if the RST IP flag has been set for that packet:

```
ip access-list extended kmdfilter1
 permit tcp any any match-any +rst
```

The following example shows how to set a permit condition for an extended access list named kmdfilter1. The access list entry specifies that a packet can pass the named access list if the RST TCP flag or the FIN TCP flag has been set for that packet:

```
ip access-list extended kmdfilter1
 permit tcp any any match-any +rst +fin
```

The following example shows how to verify the access list by using the **show access-lists** command and then to add an entry to an existing access list:

```
Router# show access-lists

Standard IP access list 1
2 permit 10.0.0.0, wildcard bits 0.0.255.255
5 permit 10.0.0.0, wildcard bits 0.0.255.255
10 permit 10.0.0.0, wildcard bits 0.0.255.255
20 permit 10.0.0.0, wildcard bits 0.0.255.255

ip access-list standard 1
 15 permit 10.0.0.0 0.0.255.255
```

The following examples shows how to remove the entry with the sequence number of 20 from the access list:

```
ip access-list standard 1
 no 20

!Verify that the list has been removed.

Router# show access-lists

Standard IP access list 1
10 permit 0.0.0.0, wildcard bits 0.0.0.255
30 permit 0.0.0.0, wildcard bits 0.0.0.255
40 permit 0.4.0.0, wildcard bits 0.0.0.255
```

The following example shows how, if a user tries to enter an entry that is a duplicate of an entry already on the list, no changes occur. The entry that the user is trying to add is a duplicate of the entry already in the access list with a sequence number of 20.

```
Router# show access-lists 101

Extended IP access list 101
    10 permit ip host 10.0.0.0 host 10.5.5.34
    20 permit icmp any any
    30 permit ip host 10.0.0.0 host 10.2.54.2
    40 permit ip host 10.0.0.0 host 10.3.32.3 log

ip access-list extended 101
```

```
 100 permit icmp any any

Router# show access-lists 101

Extended IP access list 101
    10 permit ip host 10.3.3.3 host 10.5.5.34
    20 permit icmp any any
    30 permit ip host 10.34.2.2 host 10.2.54.2
    40 permit ip host 10.3.4.31 host 10.3.32.3 log
```

The following example shows what occurs if a user tries to enter a new entry with a sequence number of 20 when an entry with a sequence number of 20 is already in the list. An error message appears, and no change is made to the access list.

```
Router# show access-lists 101

Extended IP access lists 101
    10 permit ip host 10.3.3.3 host 10.5.5.34
    20 permit icmp any any
    30 permit ip host 10.34.2.2 host 10.2.54.2
    40 permit ip host 10.3.4.31 host 10.3.32.3 log

ip access-lists extended 101
 20 permit udp host 10.1.1.1 host 10.2.2.2

%Duplicate sequence number.

Router# show access-lists 101

Extended IP access lists 101
    10 permit ip host 10.3.3.3 host 10.5.5.34
    20 permit icmp any any
    30 permit ip host 10.34.2.2 host 10.2.54.2
    40 permit ip host 10.3.4.31 host 10.3.32.3 log
```

The following example shows several **permit** statements that can be consolidated into one access list entry with noncontiguous ports. The **show access-lists** command is entered to display a group of access list entries for the access list named aaa.

```
Router# show access-lists aaa

Extended IP access lists aaa
 10 permit tcp any eq telnet any eq 450
 20 permit tcp any eq telnet any eq 679
 30 permit tcp any eq ftp any eq 450
 40 permit tcp any eq ftp any eq 679
```

Because the entries are all for the same **permit** statement and simply show different ports, they can be consolidated into one new access list entry. The following example shows the removal of the redundant access list entries and the creation of a new access list entry that consolidates the previously displayed group of access list entries:

```
ip access-list extended aaa
 no 10
 no 20
 no 30
 no 40
 permit tcp any eq telnet ftp any eq 450 679
```

The following example shows the creation of the consolidated access list entry:

```
Router# show access-lists aaa
```

```
Extended IP access list aaa
 10 permit tcp any eq telnet ftp any eq 450 679
```

The following access list filters IP packets containing Type of Service (ToS) level 3 with TTL values 10 and 20. It also filters IP packets with a TTL greater than 154 and applies that rule to noninitial fragments. It permits IP packets with a precedence level of flash and a TTL not equal to 1, and sends log messages about such packets to the console. All other packets are denied.

```
ip access-list extended canton
 deny ip any any tos 3 ttl eq 10 20
 deny ip any any ttl gt 154 fragments
 permit ip any any precedence flash ttl neq 1 log
```

The following example shows how to configure a packet filter, for any TCP source and destination, that permits communication between an OER master controller and border router:

```
ip access-list extended 100
 permit any any tcp eq drip
 exit
```

The following example shows how to set a permit condition for an extended access list named filter_logging. The access list entry specifies that a packet may pass the named access list only if it is of TCP protocol type and destined to host 10.5.5.5, all other packets are denied. In addition, the logging mechanism is enabled and one of the user defined cookies (Permit_tcp_to_10.5.5.5 or Deny_all) is appended to the appropriate syslog entry.

```
ip access-list extended filter_logging
 permit tcp any host 10.5.5.5 log Permit_tcp_to_10.5.5.5
 deny ip any any log Deny_all
```

The following example shows how to configure a packet filter for any TCP source and destination that permits inbound and outbound BGP traffic:

```
ip access-list extended 100
 permit tcp any eq bgp any eq bgp
```

Related Commands

Command	Description
absolute	Specifies an absolute time when a time range is in effect.
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
deny (IP)	Sets conditions under which a packet does not pass a named IP access list.
ip access-group	Controls access to an interface.
ip access-list log-update	Sets the threshold number of packets that cause a logging message.
ip access-list logging hash-generation	Enables hash value generation for ACE syslog entries.
ip access-list resequence	Applies sequence numbers to the access list entries in an access list.
ip options	Drops or ignores IP Options packets that are sent to the router.
logging console	Sends system logging (syslog) messages to all available TTY lines and limits messages based on severity.

Command	Description
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, or performs policy routing on packets.
periodic	Specifies a recurring (weekly) time range for functions that support the time-range feature.
show access-lists	Displays a group of access-list entries.
show ip access-list	Displays the contents of all current IP access lists.
time-range	Specifies when an access list or other feature is in effect.

permit (MAC ACL)

To set conditions for a MAC access list, use the **permit** command in MAC access-list extended configuration mode. To remove a condition from an access list, use the **no** form of this command.

permit {*src_mac_mask* | {**host name** *src_mac_name*} | **any**} {*dest_mac_mask* | {**host name** *dst_mac_name*} | **any**} [{*protocol_keyword* | {*ethertype_number ethertype_mask*}} [**vlan** *vlan_ID*] [**cos** *cos_value*]]

no permit {*src_mac_mask* | {**host name** *src_mac_name*} | **any**} {*dest_mac_mask* | {**host name** *dst_mac_name*} | **any**} [{*protocol_keyword* | {*ethertype_number ethertype_mask*}} [**vlan** *vlan_ID*] [**cos** *cos_value*]]

Syntax Description

src_mac_mask	Specifies the MAC address mask that identifies a selected block of source MAC addresses. A value of 1 represents a wildcard in that position.
host name *src_mac_name*	Specifies a source host that has been named using the **mac host name** command.
any	Specifies any source or any destination host as an abbreviation for the *src_mac_mask* or *dest_mac_mask* value of 1111.1111.1111, which declares all digits to be wildcards.
dest_mac_mask	Specifies the MAC address mask that identifies a selected block of destination MAC addresses.
host name *dst_mac_name*	Specifies a destination host that has been named using the **mac host name** command.
protocol_keyword	(Optional) Specifies a named protocol (for example, ARP).
ethertype_number	(Optional) The EtherType number specifies the protocol within the Ethernet packet.
ethertype_mask	(Optional) The EtherType mask allows a range of EtherTypes to be specified together. This is a hexadecimal number from 0 to FFFF. An EtherType mask of 0 requires an exact match of the EtherType.
vlan *vlan_ID*	(Optional) Specifies a VLAN.
cos *cos_value*	(Optional) Specifies the Layer 2 priority level for packets. The range is from 0 to 7.

Command Default

This command has no defaults.

Command Modes

MAC access-list extended configuration (config-ext-macl)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

Use this command following the **ip access-list** command to define the conditions under which a packet passes the access list.

- The **vlan** and **cos** keywords are not supported in MAC ACLs used for VACL filtering.
- The **vlan** keyword for VLAN-based QoS filtering in MAC ACLs can be globally enabled or disabled and is disabled by default.
- Enter MAC addresses as three 2-byte values in dotted hexadecimal format. For example, 0123.4567.89ab.
- Enter MAC address masks as three 2-byte values in dotted hexadecimal format. Use 1 bits as wildcards. For example, to match an address exactly, use 0000.0000.0000 (can be entered as 0.0.0).
- An entry without a protocol parameter matches any protocol.
- Enter an EtherType and an EtherType mask as hexadecimal values from 0 to FFFF.
- This list shows the EtherType values and their corresponding protocol keywords:
  - 0x0600—xns-idp—Xerox XNS IDP
  - 0x0BAD—vines-ip—Banyan VINES IP
  - 0x0baf—vines-echo—Banyan VINES Echo
  - 0x6000—etype-6000—DEC unassigned, experimental
  - 0x6001—mop-dump—DEC Maintenance Operation Protocol (MOP) Dump/Load Assistance
  - 0x6002—mop-console—DEC MOP Remote Console
  - 0x6003—decnet-iv—DEC DECnet Phase IV Route
  - 0x6004—lat—DEC Local Area Transport (LAT)
  - 0x6005—diagnostic—DEC DECnet Diagnostics
  - 0x6007—lavc-sca—DEC Local-Area VAX Cluster (LAVC), SCA
  - 0x6008—amber—DEC AMBER
  - 0x6009—mumps—DEC MUMPS
  - 0x0800—ip—Malformed, invalid, or deliberately corrupt IP frames
  - 0x8038—dec-spanning—DEC LANBridge Management
  - 0x8039—dsm—DEC DSM/DDP
  - 0x8040—netbios—DEC PATHWORKS DECnet NETBIOS Emulation
  - 0x8041—msdos—DEC Local Area System Transport
  - 0x8042—etype-8042—DEC unassigned
  - 0x809B—appletalk—Kinetics EtherTalk (AppleTalk over Ethernet)
  - 0x80F3—aarp—Kinetics AppleTalk Address Resolution Protocol (AARP)

Examples

This example shows how to create a MAC-Layer ACL named mac_layer that permits dec-phase-iv traffic with source address 0000.4700.0001 and destination address 0000.4700.0009, but denies all other traffic:

```
Router(config)# mac access-list extended mac_layer
Router(config-ext-macl)# permit 0000.4700.0001 0.0.0 0000.4700.0009 0.0.0 dec-phase-iv
Router(config-ext-macl)# deny any any
```

Related Commands

Command	Description
deny (MAC ACL)	Sets deny conditions for a named MAC access list.
mac access-list extended	Defines a MAC access list by name.
mac host	Assigns a name to a MAC address.
show mac access-group	Displays the contents of all current MAC access groups.

permit (reflexive)

To create a reflexive access list and to enable its temporary entries to be automatically generated, use the **permit** command in access-list configuration mode. To delete the reflexive access list (if only one protocol was defined) or to delete protocol entries from the reflexive access list (if multiple protocols are defined), use the **no** form of this command.

permit *protocol source source-wildcard destination destination-wildcard* **reflect** *name* [**timeout** *seconds*]

no permit *protocol source-wildcard destination destination-wildcard* **reflect** *name*

Syntax Description

protocol	Name or number of an IP protocol. It can be one of the keywords **gre**, **icmp**, **ip**, **ipinip**, **nos**, **tcp**, or **udp**, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including Internet Control Message Protocol, Transmission Control Protocol, and User Datagram Protocol), use the keyword **ip**.
source	Number of the network or host from which the packet is being sent. There are three other ways to specify the source: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. This keyword is normally not recommended (see the section "Usage Guidelines"). • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
source-wildcard	Wildcard bits (mask) to be applied to source. There are three other ways to specify the source wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. This keyword is normally not recommended (see the section "Usage Guidelines"). • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
destination	Number of the network or host to which the packet is being sent. There are three other ways to specify the destination: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the keyword **any** as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. This keyword is normally *not* recommended (see the section "Usage Guidelines"). • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of destination 0.0.0.0.

destination-wildcard	Wildcard bits to be applied to the destination. There are three other ways to specify the destination wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the keyword **any** as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. This keyword is normally *not* recommended (see the section "Usage Guidelines"). • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
reflect	Identifies this access list as a reflexive access list.
name	Specifies the name of the reflexive access list. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists. The name can be up to 64 characters long.
timeout *seconds*	(Optional) Specifies the number of seconds to wait (when no session traffic is being detected) before entries expire in this reflexive access list. Use a positive integer from 0 to 2^{32}–1. If not specified, the number of seconds defaults to the global timeout value.

Defaults

If this command is not configured, no reflexive access lists will exist, and no session filtering will occur.

If this command is configured without specifying a **timeout** value, entries in this reflexive access list will expire after the global timeout period.

Command Modes

Access-list configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is used to achieve reflexive filtering, a form of session filtering.

For this command to work, you must also nest the reflexive access list using the **evaluate** command.

This command creates a reflexive access list and triggers the creation of entries in the same reflexive access list. This command must be an entry (condition statement) in an extended named IP access list.

If you are configuring reflexive access lists for an external interface, the extended named IP access list should be one which is applied to outbound traffic.

If you are configuring reflexive access lists for an internal interface, the extended named IP access list should be one which is applied to inbound traffic.

IP sessions that originate from within your network are initiated with a packet exiting your network. When such a packet is evaluated against the statements in the extended named IP access list, the packet is also evaluated against this reflexive **permit** entry.

As with all access list entries, the order of entries is important, because they are evaluated in sequential order. When an IP packet reaches the interface, it will be evaluated sequentially by each entry in the access list until a match occurs.

If the packet matches an entry prior to the reflexive **permit** entry, the packet will not be evaluated by the reflexive **permit** entry, and no temporary entry will be created for the reflexive access list (session filtering will not be triggered).

The packet will be evaluated by the reflexive **permit** entry if no other match occurs first. Then, if the packet matches the protocol specified in the reflexive **permit** entry, the packet is forwarded and a corresponding temporary entry is created in the reflexive access list (unless the corresponding entry already exists, indicating the packet belongs to a session in progress). The temporary entry specifies criteria that permits traffic into your network only for the same session.

Characteristics of Reflexive Access List Entries

This command enables the creation of temporary entries in the same reflexive access list that was defined by this command. The temporary entries are created when a packet exiting your network matches the protocol specified in this command. (The packet "triggers" the creation of a temporary entry.) These entries have the following characteristics:

- The entry is a **permit** entry.
- The entry specifies the same IP upper-layer protocol as the original triggering packet.
- The entry specifies the same source and destination addresses as the original triggering packet, except the addresses are swapped.
- If the original triggering packet is TCP or UDP, the entry specifies the same source and destination port numbers as the original packet, except the port numbers are swapped.

  If the original triggering packet is a protocol other than TCP or UDP, port numbers do not apply, and other criteria are specified. For example, for ICMP, type numbers are used: the temporary entry specifies the same type number as the original packet (with only one exception: if the original ICMP packet is type 8, the returning ICMP packet must be type 0 to be matched).
- The entry inherits all the values of the original triggering packet, with exceptions only as noted in the previous four bullets.
- IP traffic entering your internal network will be evaluated against the entry, until the entry expires. If an IP packet matches the entry, the packet will be forwarded into your network.
- The entry will expire (be removed) after the last packet of the session is matched.
- If no packets belonging to the session are detected for a configurable length of time (the timeout period), the entry will expire.

Examples

The following example defines a reflexive access list *tcptraffic*, in an outbound access list that permits all Border Gateway Protocol and Enhanced Interior Gateway Routing Protocol traffic and denies all ICMP traffic. This example is for an external interface (an interface connecting to an external network).

First, the interface is defined and the access list is applied to the interface for outbound traffic.

```
interface Serial 1
 description Access to the Internet via this interface
 ip access-group outboundfilters out
```

Next, the outbound access list is defined and the reflexive access list *tcptraffic* is created with a reflexive **permit** entry.

```
ip access-list extended outboundfilters
 permit tcp any any reflect tcptraffic
```

Related Commands

Command	Description
evaluate	Nests a reflexive access list within an access list.
ip access-list	Defines an IP access list by name.
ip reflexive-list timeout	Specifies the length of time that reflexive access list entries will continue to exist when no packets in the session are detected.

permit (webvpn acl)

To set conditions to allow packets to pass a named Secure Sockets Layer Virtual Private Network (SSL VPN) access list, use the **permit** command in webvpn acl configuration mode. To remove a permit condition from an access list, use the **no** form of this command.

permit [**url** [**any** | *url-string*]] [**ip** | **tcp** | **udp** | **http** | **https** | **cifs**] [**any** | *source-ip source-mask*] [**any** | *destination-ip destination-mask*] **time-range** *time-range-name* [**syslog**]

no permit url [**any** | *url-string*] [**ip** | **tcp** | **udp** | **http** | **https** | **cifs**] [**any** | *source-ip source-mask*] [**any** | *destination-ip destination-mask*] **time-range** *time-range-name* [**syslog**]

Syntax Description

url	(Optional) Filtering rules are applied to a URL. • Use the **any** keyword as an abbreviation for any URL.
url-string	(Optional) URL string defined as follows: **scheme://host[:port][/path]** • **scheme**—Can be HTTP, Secure HTTPS (HTTPS), or Common Internet File System (CIFS). This field is required in the URL string. • **host**—Can be a hostname or a host IP (host mask). The host can have one wildcard (*). • **port**—Can be any valid port number (1–65535). It is possible to have multiple port numbers separated by a comma (,). The port range is expressed using a dash (-). • **path**—Can be any valid path string. In the path string, the $user is translated to the current user name.
ip	(Optional) Permits only IP packets. When you enter the **ip** keyword, you must use the specific command syntax shown for the IP form of the **permit** command.
tcp	(Optional) Permits only TCP packets. When you enter the **tcp** keyword, you must use the specific command syntax shown for the TCP form of the **permit** command.
udp	(Optional) Permitss only UDP packets. When you enter the **udp** keyword, you must use the specific command syntax shown for the UDP form of the **permit** command.
http	(Optional) Permits only HTTP packets. When you enter the **http** keyword, you must use the specific command syntax shown for the HTTP form of the **permit** command.
https	(Optional) Permits only HTTPS packets. When you enter the **https** keyword, you must use the specific command syntax shown for the HTTPS form of the **permit** command.
cifs	(Optional) Permits only CIFS packets. When you enter the **cifs** keyword, you must use the specific command syntax shown for the CIFS form of the **permit** command.

source-ip source-mask	(Optional) Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for a source and source mask of 0.0.0.0 255.255.255.255. • Use **host** source as an abbreviation for a source and source-wildcard of source 0.0.0.0.
destination-ip destination-mask	(Optional) Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for a source and source mask of 0.0.0.0 255.255.255.255. • Use **host** source as an abbreviation for a source and source-wildcard of source 0.0.0.0.
time-range *time-range-name*	Name of the time range that applies to this **permit** statement. The name of the time range and its restrictions are specified by the **time-range** and **absolute** or **periodic** commands, respectively.
syslog	(Optional) System logging messages are generated.

Command Default

All packets are permitted.

Command Modes

Webvpn acl configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use this command following the **acl** command (in webvpn context configuration mode) to specify conditions under which a packet can pass the named access list.

The **time-range** keyword allows you to identify a time range by name. The **time-range**, **absolute**, and **periodic** commands specify when this permit statement is in effect.

Examples

The following example shows that all packets from the URL "https://10.168.2.228:34,80-90,100-/public" are permitted to pass ACL "acl1":

```
webvpn context context1
 acl acl1
  permit url "https://10.168.2.228:34,80-90,100-/public"
```

Related Commands

Command	Description
absolute	Specifies an absolute time for a time range.
deny (webvpn acl)	Sets conditions in a named SSL VPN access list that will deny packets.
periodic	Specifies a recurring (weekly) time range for functions that support the time-range feature.
time-range	Enables time-range configuration mode and defines time ranges for extended access lists.

pfs

To configure a server to notify the client of the central-site policy regarding whether PFS is required for any IP Security (IPSec) Security Association (SA), use the **pfs** command in global configuration mode. To restore the default behavior, use the **no** form of this command.

pfs

no pfs

Syntax Description

This command has no arguments or keywords.

Defaults

The server will not notify the client of the central-site policy regarding whether PFS is required for any IPSec SA.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

Before you use the **pfs** command, you must first configure the **crypto isakmp client configuration group** command.

An example of an attribute-value (AV) pair for the PFS attribute is as follows:

```
ipsec:pfs=1
```

Examples

The following example shows that the server has been configured to notify the client of the central-site policy regarding whether PFS is required for any IPSec SA:

```
crypto isakmp client configuration group
 pfs
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.

pki-server

To specify the certificate server that is to be associated with the Trusted Transitive Introduction (TTI) exchange between the Secure Device Provisioning (SDP) petitioner and the SDP registrar, use the **pki-server** command in tti-registrar configuration mode. To change the specified certificate server, use the **no** form of this command.

pki-server *label*

no pki-server *label*

Syntax Description

label	Name of certificate server.

Defaults

A certificate server is not associated with the TTI exchange; thus, the petitioner and registrar will not be able to communicate.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Although any device that contains a crypto image can be the registrar, it is recommended that the registrar be either a Cisco IOS certificate server registration authority (RA) or a Cisco IOS certificate server root.

Examples

The following example shows how to associate the certificate server "cs1" with the TTI exchange:

```
crypto wui tti registrar
 pki-server cs1
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.
crypto wui tti registrar	Configures a device to become an SDP registrar and enters tti-registrar configuration mode.

pki trustpoint

To use the PKI trustpoints in the Rivest, Shamir and Adleman (RSA) signature authentication method, use the **pki trustpoint** command in IKEv2 profile configuration mode. To remove the trustpoint, use the **no** form of this command.

pki trust-point *trustpoint-name* [**sign** | **verify**]

no pki trust-point *trustpoint-name* [**sign** | **verify**]

Syntax Description

trustpoint-name	The trustpoint name as defined in the global configuration.
sign	(Optional) Uses certificates from the trustpoint to create a digital signature that is sent to the peer.
verify	(Optional) Uses certificates from the trustpoint to validate digital signatures received from thepeer.

Command Default

If there is no trustpoint defined in the IKEv2 profile configuration, the default is to validate the certificate using all the trustpoints that are defined in the global configuration.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

The **pki trustpoint** command specifies the trustpoints that are used with the RSA-signature authentication method. You can configure upto six truspoints.

Note If the **sign** or **verify** keyword is not specified, the trustpoint is used for signing and verification.

Examples

The following example specifies two trustpoints, trustpoint-local for local authentication using sign and trustpoint-remote for remote verification using verify:

```
Router(config)# crypto ikev2 profile profile2
Router(config-ikev2-profile)# pki trustpoint trustpoint-local sign
Router(config-ikev2-profile)# pki trustpoint trustpoint-remote verify
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.

police (zone policy)

To limit traffic matching within a firewall (inspect) policy, use the **police** command in policy-map-class configuration mode. To remove traffic limiting from the firewall policy configuration, use the **no** form of this command.

police rate *bps* [**burst** *size*]

no police rate *bps* [**burst** *size*]

Syntax Description

rate *bps*	Average rate in bits per second (bps). Valid values are 8000 to 2000000000. **Note** Traffic limiting is in bps only; that is, packets per seconds (pps) and percent rates are not supported.
burst *size*	(Optional) Burst size in bytes. Valid values are 1000 to 51200000. The default normal burst size is 1500 bytes.

Command Default

Traffic limiting is disabled.

Command Modes

Policy-map-class configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Issue the **police** command within an inspect policy to limit the number of concurrent connections allowed for applications such as Instant Messenger (IM) and peer-to-peer (P2P).

To effectively use the **police** command, you must also enable Cisco IOS stateful packet inspection within the inspect policy map. If you configure the **police** command without configuring the inspect action (via the **inspect** command), you will receive an error message and the **police** command will be rejected.

Because an inspect policy map can be applied only to a zone pair, and not an interface, the police action will be enforced on traffic that traverses the zone pair. (The direction is inherent to the specification of the zone pair.)

The police action is not allowed in policies that are attached to zone pairs involving a “self” zone. If you want to perform this task, you should use control plane policing.

Examples

The following example shows how to limit traffic matching with the inspect policy “p1”:

```
policy-map type inspect p1
 class type inspect c1
  inspect
  police rate 1000 burst 6100
```

The following example is sample output from the s**how policy-map type inspect zone-pair** command, which can now be used to verify the police action configuration:

```
Router# show policy-map type inspect zone-pair

Zone-pair: zp

Service-policy inspect : test-udp

  Class-map: check-udp (match-all)
   Match: protocol udp
   Inspect
    Packet inspection statistics [process switch:fast switch]
    udp packets: [3:4454]

    Session creations since subsystem startup or last reset 92
    Current session counts (estab/half-open/terminating) [5:33:0]
    Maxever session counts (estab/half-open/terminating) [5:59:0]
    Last session created 00:00:06
    Last statistic reset never
    Last session creation rate 61
    Last half-open session total 33
   Police
   rate 8000 bps,1000 limit
   conformed 2327 packets, 139620 bytes; actions: transmit
   exceeded 36601 packets, 2196060 bytes; actions: drop
   conformed 6000 bps, exceed 61000 bps

  Class-map: class-default (match-any)
   Match: any
   Drop (default action)
   0 packets, 0 bytes
```

Related Commands

Command	Description
show policy-map type inspect zone-pair	Displays the runtime inspect type policy map statistics and other information such as sessions existing on a specified zone pair.

policy

To define the Central Policy Push (CPP) firewall policy push, use the command in global configuration mode. To remove the CPP policy that was configured, use the **no** form of this command.

policy {**check-presence** | **central-policy-push** {**access-list** {**in** | **out**} {*access-list-name* | *access-list-number*}}

no policy {**check-presence** | **central-policy-push** {**access-list** {**in** | **out**} {*access-list-name* | *access-list-number*}}

Syntax Description

check-presence	Instructs the server to check for the presence of the specified firewall as shown as *firewall-type* on the client.
central-policy-push	Pushes the CPP firewall policy push. The configuration following this keyword specifies the actual policy, such as the input and output access lists that have to be applied by the client firewall of the type *firewall-type*.
access-list in	Defines the inbound access list on the virtual private network (VPN) remote client.
access-list out	Defines the outbound access list on the VPN remote client.
access-list-name | *access-list-number*	Access list name or number.

Command Default

The CPP policy is not defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Examples

The following example defines the CPP policy name as “hw-client-g-cpp.” The “Cisco-Security-Agent” policy type is mandatory. The CPP inbound list is “192” and the outbound list is “sample”:

```
crypto isakmp client firewall hw-client-g-cpp required Cisco-Security-Agent
 policy central-policy-push access-list in 192
 policy central-policy-push access-list out sample
 policy check-presence:
```

The following example shows access lists that have been applied on a VPN remote client and later applied by the client firewall :

Defines the inbound access control list that is applied on the VPN remote client

.
.
.

```
access-list 170 permit ip 172.18.124.0 0.0.0.255 any
access-list 170 permit ip 172.21.1.0 0.0.0.255 any
.
.
.
```

Defines the outbound ACL that is applied on the VPN remote client

```
.
.
.
access-list 180 permit ip any 172.18.124.0 0.0.0.255
.
.
.
```

Inbound and outbound policies to be applied by the client firewall

```
.
.
.
crypto isakmp client firewall test required cisco-integrated-client-firewall
  policy central-policy-push access-list in 170
  policy central-policy-push access-list out 180
.
.
.
crypto isakmp client configuration group vpngroup1
  firewall policy test
.
.
.
```

Related Commands

Command	Description
crypto isakmp client firewall	Defines the CPP) firewall push policy on a server.

policy group

To enter webvpn group policy configuration mode to configure a group policy, use the **policy group** command in webvpn context configuration mode. To remove the policy group from the router configuration file, use the **no** form of this command.

policy group *name*

no policy group *name*

Syntax Description

name	Name of the policy group.

Command Default

Webvpn group policy configuration mode is not entered, and a policy group is not configured.

Command Modes

Webvpn context configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The policy group is a container that defines the presentation of the portal and the permissions for resources that are configured for a group of end users. Entering the **policy group** command places the router in webvpn group policy configuration mode. After the group policy is configured, the policy group is attached to the SSL VPN context configuration by configuring the **default-group-policy** command.

Examples

The following example configures a policy group named ONE:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# exit
Router(config-webvpn-context)# default-group-policy ONE
```

Related Commands

Command	Description
banner	Configures a banner to be displayed after a successful login.
citrix enabled	Enables Citrix application support for end users in a policy group.
default-group-policy	Configures a default group policy for SSL VPN sessions.
filter citrix	Configures a Citrix application access filter.
filter tunnel	Configures a SSL VPN tunnel access filter.
functions	Enables a file access function or tunnel mode support in a group policy configuration.
hide-url-bar	Prevents the URL bar from being displayed on the SSL VPN portal page.

Command	Description
nbns-list (policy group)	Attaches a NBNS server list to a policy group configuration.
port-forward (policy group)	Attaches a port-forwarding list to a policy group configuration.
svc address-pool	Configures a pool of IP addresses to assign to end users in a policy group.
svc default-domain	Configures the domain for a policy group.
svc dns-server	Configures DNS servers for policy group end users.
svc dpd-interval	Configures the DPD timer value for the gateway or client.
svc homepage	Configures the URL of the web page that is displayed upon successful user login.
svc keep-client-installed	Configures the end user to keep Cisco AnyConnect VPN Client software installed when the SSL VPN connection is not enabled.
svc msie-proxy	Configures MSIE browser proxy settings for policy group end users.
svc msie-proxy server	Specifies a Microsoft Internet Explorer proxy server for policy group end users.
svc rekey	Configures the time and method that a tunnel key is refreshed for policy group end users.
svc split	Configures split tunneling for policy group end users.
svc wins-server	Configures configure WINS servers for policy group end users.
timeout	Configures the length of time that an end user session can remain idle or the total length of time that the session can remain connected.
url-list (policy group)	Attaches a URL list to policy group configuration.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

policy-map type inspect

To create a Layer 3 and Layer 4 or a Layer 7 (protocol-specific) inspect type policy map, use the **policy-map type inspect** command in global configuration mode. To delete an inspect type policy map, use the **no** form of this command.

Layer 3 and Layer 4 (Top Level) Policy Map Syntax

policy-map type inspect *policy-map-name*

no policy-map type inspect *policy-map-name*

Layer 7 (Application-Specific) Policy Map Syntax

policy-map type inspect *protocol-name policy-map-name*

no policy-map type inspect *protocol-name policy-map-name*

Syntax Description

policy-map-name	Name of the policy map. The name can be a maximum of 40 alphanumeric characters.
protocol-name	Layer 7 application-specific policy map. The supported protocols are as follows: • **h323**—H.323 protocol, Version 4 • **http**—HTTP • **im**—Instant Messenger (IM) protocol For **im**, the supported IM protocols include: – AOL Version 5 and later versions – I Seek You (ICQ) Version 2003b.5.56.1.3916.85 – MSN Messenger Version 6.x and 7.x – Windows Messenger Version 5.1.0701 – Yahoo Messenger Version 9.0 and later versions • **imap**—Internet Message Access Protocol (IMAP) • **p2p**—Peer-to-peer (P2P) protocol • **pop3**—Post Office Protocol, Version 3 (POP3) • **sip**—Session Initiation Protocol (SIP) • **smtp**—Simple Mail Transfer Protocol (SMTP) • **sunrpc**—Sun Remote Procedure Call (SUNRPC)

Command Default

No policy-map is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(9)T	Support for the following protocols and keywords was added: • P2P protocol and the **p2p** keyword • IM protocol and the **im** keyword
12.4(15)XZ	This command was integrated into Cisco IOS Release 12.4(15)XZ. Support for the SIP protocol was added.
12.4(20)T	Support for the ICQ and Windows Messenger IM protocols and following keywords was added: **icq**, **winmsgr** Support for the H.323 VoIP protocol and following keyword was added: **h323**

Usage Guidelines

Use the **policy-map type inspect** command to create a Layer 3, Layer 4 inspect type policy map or a Layer 7 application-specific inspect type policy map. After you create a policy map, you should enter the **class type inspect** command (as appropriate for your configuration) to specify the traffic (class) on which an action is to be performed. The class was previously defined in a class map. Thereafter, you should enter the **inspect** command to enable Cisco IOS stateful packet inspection and to specify inspect-specific parameters in a parameter map.

Layer 3, Layer 4 (Top Level) Policy Maps

Top-level policy maps allow you to define high-level actions such as **inspect**, **drop**, **pass**, and **urlfilter**. You can attach the maps to a target (zone pair). The maps can contain "child" policies that are also known as application-specific Layer 7 policies.

Layer 7 (Application-Specific) Policy Maps

Application-specific policy maps are used to specify a policy for an application protocol. For example, if you want to drop HTTP traffic with Uniform Resource Identifier (URI) lengths exceeding 256 bytes, you must configure an HTTP policy map to do that. Application-specific policy maps cannot be attached directly to a target (zone pair). They must be configured as "child" policies in a top-level Layer 3 or Layer 4 policy map.

Examples

The following example specifies the traffic class (host) on which the drop action is to be performed:

```
policy-map type inspect mypolicy
 class type inspect host
 drop
```

The following example shows how to configure the policy map "my-im-pmap" with two IM classes—AOL and Yahoo Messenger—and allow only text-chat messages to pass through. When any packet with a service other than "text-chat" is seen, the connection will be reset.

```
class-map type inspect aol match-any my-aol-cmap
 match service text-chat
!
class-map type inspect ymsgr match-any my-ysmgr-cmap
 match service any
!
policy-map type inspect im my-im-pmap
 class type inspect aol my-aol-cmap
 allow
```

```
 log
!
 class type inspect ymsgr my-ysmgr-cmap
 reset
 log
```

Related Commands

Command	Description
class type inspect	Specifies the traffic (class) on which an action is to be performed.

policy-map type inspect urlfilter

To create or modify a URL filter type inspect policy map, use the **policy-map type inspect urlfilter** command in global configuration mode. To delete a URL filter type inspect policy map, use the **no** form of this command.

policy-map type inspect urlfilter *policy-map-name*

no policy-map type inspect urlfilter *policy-map-name*

Syntax Description

policy-map-name	Name of the policy map.

Command Default

No policy map is created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **policy-map type inspect urlfilter** command to create a URL filter type inspect policy map. The policy map specifies the traffic (**class type urlfilter**) and the actions to be performed on that traffic for the specified URL filtering policy.

Before you create a URL filter type inspect policy map, use the following commands:

- **class-map type urlfilter** command to configure the match criteria for the traffic.
- **parameter-map type urlfpolicy** command to specify the parameters for the URL filtering server. If you are configuring a policy for a Trend Router Provisioning Server (TRPS), you must also specify the global filtering parameters with the **parameter-map type trend-global** command.

After you create a policy map, use the following commands to configure the URL filtering policy:

- **class type urlfilter** [**trend** | **n2h2** | **websense**] *class-name*—Specifies the class of traffic to which the policy applies. If you specify an optional URL filtering server, you must also use the **parameter type urlfpolicy** command to specify the appropriate per-policy parameters for that URL filtering server.

  For each class, use one of the URL filtering action commands to specify how to handle a URL that matches the class map. Table 53 lists the URL filtering action commands.

Table 53 URL Filtering Action Commands

Command	Description
allow	Permits access to the requested URL.
log	Logs the URL request.

Table 53 URL Filtering Action Commands

Command	Description
reset	Resets the HTTP connection at both ends.
server-specified action	Specifies that the traffic is handled by the URL filtering server. This action is valid only for Websense and N2H2 classes.

- **description** *string*—Describes the policy.
- **exit**—Exits the policy map.
- **no**—Negates or sets the default value for a command.
- **parameter type urlfpolicy** [**trend | n2h2 | websense**]—Specifies what type of URL filtering this policy applies to: local (default), Trend Micro, SmartFilter, or Websense.
- **rename** *policy-map-name*—Specifies a new name for the policy map.

Examples

The following example shows a how to create a URL filter type inspect policy for a Trend Micro URL filtering server. The policy logs URL requests that match the URL categories specified in the class drop-category, and then resets the connection, thus denying the request.

```
class-map type urlfilter trend match-any drop-category
 match url category Gambling
 match url category Personals-Dating

parameter-map type trend-global global-parameter-map
 server trend.example.com

parameter-map type urlfpolicy trend g1-trend-pm
 max-request 2147483647
 max-resp-pak 20000
 allow-mode on
 truncate hostname
 block-page message "group1: 10.10.10.0 is blocked by Trend."

policy-map type inspect urlfilter g1-trend-policy
 parameter type urlfpolicy trend g1-trend-parameter-map
 class type urlfilter trend drop-category
  log
 reset
```

The following example shows a filtering policy for a Websense URL filtering server. The policy logs and allows URL requests that are in the trusted domain class, logs and denies URL requests that are in the untrusted domain class, and logs and denies URL requests that are in the keyword class.

```
policy-map type inspect urlfilter websense-policy
 parameter type urlfpolicy websense websense-parameter-map
 class type urlfilter trusted-domain-class
  log
  allow
 class type urlfilter untrusted-domain-class
  log
  reset
 class type urlfilter keyword-class
  log
  reset
```

Related Commands

Command	Description
class-map type urlfilter	Specifies the class on which a policy action is to be performed.
class type urlfilter	Associates a URL filter class map with a URL filtering policy maps.
parameter-map type trend-global	Creates or modifies the parameter map for global TRPS parameters.
parameter-map type urlfpolicy	Creates or modifies a parameter map for a URL filtering policy.

pool (isakmp-group)

To define a local pool address, use the **pool** command in ISAKMP group configuration mode or IKEv2 authorization policy configuration mode. To remove a local pool from your configuration, use the **no** form of this command.

pool *name*

no pool *name*

Syntax Description

name	Name of the local address pool.

Defaults

No local pool address is defined.

Command Modes

ISAKMP group configuration (config-isakmp-group)
IKEv2 authorization policy configuration (config-ikev2-author-policy)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use the **pool** command to refer to an IP local pool address, which defines a range of addresses that will be used to allocate an internal IP address to a client. Although a user must define at least one pool name, a separate pool may be defined for each group policy.

Note This command must be defined and refer to a valid IP local pool address, or the client connection will fail.

You must enable the following commands before enabling the **dns** command:

- **crypto isakmp client configuration group**—Specifies the group policy information that has to be defined or changed.
- **crypto ikev2 authorization policy**—Specifies the local group policy authorization parameters.

Examples

The following example shows how to refer to the local pool address “dog”:

```
crypto isakmp client configuration group cisco
```

```
  key cisco
  dns 10.2.2.2 10.3.2.3
  pool dog
  acl 199
!
ip local pool dog 10.1.1.1 10.1.1.254
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto ikev2 authorization policy	Specifies an IKEv2 authorization policy group.
crypto isakmp client configuration group	Specifies the DNS domain to which a group belongs.
ip local pool	Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.

port

To specify the port on which a device listens for RADIUS requests from configured RADIUS clients, use the **port** command in dynamic authorization local server configuration mode. To restore the default, use the **no** form of this command.

port *port-number*

no port *port-number*

Syntax Description

port-number	Port number. The default value is port 1700.

Command Default

The device listens for RADIUS requests on the default port (port 1700).

Command Modes

Dynamic authorization local server configuration (config-locsvr-da-radius)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

A device (such as a router) can be configured to allow an external policy server to dynamically send updates to the router. This functionality is facilitated by the CoA RADIUS extension. CoA introduced peer-to-peer capability to RADIUS, enabling a router and external policy server each to act as a RADIUS client and server. Use the **port** command to specify the ports on which the router will listen for requests from RADIUS clients.

Examples

The following example specifies port 1650 as the port on which the device listens for RADIUS requests:

```
aaa server radius dynamic-author
 client 10.0.0.1
 port 1650
```

Related Commands

Command	Description
aaa server radius dynamic-author	Configures a device as a AAA server to facilitate interaction with an external policy server.

port-forward

To enter webvpn port-forward list configuration mode to configure a port-forwarding list, use the **port-forward** command in webvpn context configuration mode. To remove the port-forwarding list from the SSL VPN context configuration, use the **no** form of this command.

port-forward *name*

no port-forward *name*

Syntax Description

name	Name of the port-forwarding list.

Command Default

Webvpn port-forward list configuration mode is not entered, and a port-forwarding list is not configured.

Command Modes

Webvpn context configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The **port-forward** command is used to create the port-forwarding list. Application port number mapping (port forwarding) is configured with the **local-port** command in webvpn port-forward configuration mode.

A port-forwarding list is configured for thin client mode SSL VPN. Port forwarding extends the cryptographic functions of the SSL-protected browser to provide remote access to TCP-based applications that use well-known port numbers, such as POP3, SMTP, IMAP, Telnet, and SSH.

When port forwarding is enabled, the hosts file on the SSL VPN client is modified to map the application to the port number configured in the forwarding list. The application port mapping is restored to default when the user terminates the SSL VPN session.

Examples

The following example configures port forwarding for well-known e-mail application port numbers:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# port-forward EMAIL
Router(config-webvpn-port-fwd)# local-port 30016 remote-server mail.company.com
remote-port 110 description POP3
Router(config-webvpn-port-fwd)# local-port 30017 remote-server mail.company.com
remote-port 25 description SMTP
Router(config-webvpn-port-fwd)# local-port 30018 remote-server mail.company.com
remote-port 143 description IMAP
```

Related Commands

Command	Description
local-port (WebVPN)	Remaps an application port number in a port-forwarding list.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

port-forward (policy group)

To attach a port-forwarding list to a policy group configuration, use the **port-forward** command in webvpn group policy configuration mode. To remove the port-forwarding list from the policy group configuration, use the **no** form of this command.

port-forward *name* [**auto-download** [**http-proxy** [**proxy-url** *homepage-url*]] | **http-proxy** [**proxy-url** *homepage-url*] [**auto-download**]]

no port-forward *name* [**auto-download** [**http-proxy** [**proxy-url** *homepage-url*]] | **http-proxy** [**proxy-url** *homepage-url*] [**auto-download**]]

Syntax Description

name	Name of the port-forwarding list that was configured in webvpn context configuration mode.
auto-download	(Optional) Allows for automatic download of the port-forwarding Java applet on the portal page of a website.
http-proxy	(Optional) Allows the Java applet to act as a proxy for the browser of the user.
proxy-url *homepage-url*	(Optional) Page at this URL address opens as the portal page of the user.

Command Default

A port-forwarding list is not attached to a policy group configuration.

Command Modes

Webvpn group policy configuration (config-webvpn-group)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(9)T	This command was modified. The **auto-download** keyword was added.

Usage Guidelines

The configuration of this command applies to only clientless access mode. In clientless mode, the remote user accesses the internal or corporate network using the web browser on the client machine.

Examples

The following example shows how to apply the port-forwarding list to the policy group configuration:

```
webvpn context context1
 port-forward EMAIL
  local-port 30016 remote-server mail.company.com remote-port 110 description POP3
  local-port 30017 remote-server mail.company.com remote-port 25 description SMTP
  local-port 30018 remote-server mail.company.com remote-port 143 description IMAP
  exit
 policy group ONE
 port-forward EMAIL auto-download
```

The following example shows that HTTP proxy has been configured. The page at URL "http://www.example.com" will automatically download as the home page of the user.

```
webvpn context myContext
 ssl authenticate verify all
 !
 !
 port-forward "email"
   local-port 20016 remote-server "ssl-server1.sslvpn-ios.com" remote-port 110 description
"POP-ssl-server1"
 !
 policy group myPolicy
   port-forward "email" auto-download http-proxy proxy-url "http://www.example.com"
 inservice
```

Related Commands

Command	Description
local-port (WebVPN)	Remaps an application port number in a port-forwarding list.
policy group	Enters webvpn group policy configuration mode to configure a group policy.
port-forward	Enters webvpn port-forward list configuration mode to configure a port-forwarding list.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

port-misuse

To permit or deny HTTP traffic through the firewall on the basis of specified applications in the HTTP message, use the **port-misuse** command in appfw-policy-http configuration mode. To disable this inspection parameter, use the **no** form of this command.

port-misuse {**p2p** | **tunneling** | **im** | **default**} **action** {**reset** | **allow**} [**alarm**]

no port-misuse {**p2p** | **tunneling** | **im** | **default**} **action** {**reset** | **allow**} [**alarm**]

Syntax Description

p2p	Peer-to-peer protocol applications subject to inspection: Kazaa and Gnutella.
tunneling	Tunneling applications subject to inspection: HTTPPort/HTTPHost, GNU Httptunnel, GotoMyPC, Firethru, Http-tunnel.com Client
im	Instant messaging protocol applications subject to inspection: Yahoo Messenger.
default	All applications are subject to inspection.
action	Applications detected within the HTTP messages that are outside of the specified application are subject to the specified action (**reset** or **allow**).
reset	Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection.
allow	Forwards the packet through the firewall.
alarm	(Optional) Generates system logging (syslog) messages for the given action.

Defaults

If this command is not enabled, HTTP messages are permitted through the firewall if any of the applications are detected within the message.

Command Modes

appfw-policy-http configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

The following example shows how to define the HTTP application firewall policy “mypolicy.” This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule “firewall,” which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
```

```
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

ppp accounting

To enable authentication, authorization, and accounting (AAA) accounting services on the selected interface, use the **ppp accounting** command in interface configuration mode. To disable AAA accounting services, use the **no** form of this command.

ppp accounting default

no ppp accounting

Syntax Description

default	The name of the method list is created with the **aaa accounting** command.

Defaults

Accounting is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

After you enable the **aaa accounting** command and define a named accounting method list (or use the default method list), you must apply the defined lists to the appropriate interfaces for accounting services to take place. Use the **ppp accounting** command to apply the specified method lists (or if none is specified, the default method list) to the selected interface.

Examples

The following example enables accounting on asynchronous interface 4 and uses the accounting method list named charlie:

```
interface async 4
 encapsulation ppp
 ppp accounting charlie
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.

ppp authentication

To enable at least one PPP authentication protocol and to specify the order in which the protocols are selected on the interface, use the **ppp authentication** command in interface configuration mode. To disable this authentication, use the **no** form of this command.

ppp authentication {*protocol1* [*protocol2...*]} [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] [**optional**]

no ppp authentication

Syntax Description

protocol1 [*protocol2...*]	At least one of the keywords described in Table 54.
if-needed	(Optional) Used with TACACS and extended TACACS. Does not perform Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) authentication if authentication has already been provided. This option is available only on asynchronous interfaces.
list-name	(Optional) Used with authentication, authorization, and accounting (AAA). Specifies the name of a list of methods of authentication to use. If no list name is specified, the system uses the default. The list is created with the **aaa authentication ppp** command.
default	(Optional) Name of the method list created with the **aaa authentication ppp** command.
callin	(Optional) Authentication on incoming (received) calls only.
one-time	(Optional) The username and password are accepted in the username field.
optional	(Optional) Accepts the connection even if the peer refuses to accept the authentication methods that the router has requested.

Defaults

PPP authentication is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1(1)	The **optional** keyword was added.
12.1(3)XS	The **optional** keyword was added.
12.2(2)XB5	Support for the **eap** authentication protocol was added on the Cisco 2650, Cisco 3640, Cisco 3660, Cisco AS5300, and Cisco AS5400 platforms.
12.2(13)T	The **eap** authentication protocol support introduced in Cisco IOS Release 12.2(2)XB5 was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When you enable Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), or Extensible Authentication Protocol (EAP) authentication (or all three methods), the local router requires the remote device to prove its identity before allowing data traffic to flow. PAP authentication requires the remote device to send a name and a password, which is checked against a matching entry in the local username database or in the remote security server database. CHAP authentication sends a challenge message to the remote device. The remote device encrypts the challenge value with a shared secret and returns the encrypted value and its name to the local router in a Response message. The local router attempts to match the name of the remote device with an associated secret stored in the local username or remote security server database; it uses the stored secret to encrypt the original challenge and verify that the encrypted values match. EAP works much as CHAP does, except that identity request and response packets are exchanged when EAP starts.

You can enable CHAP, Microsoft CHAP (MS-CHAP), PAP, or EAP in any order. If you enable all four methods, the first method specified is requested during link negotiation. If the peer suggests using the second method, or refuses the first method, the second method is tried. Some remote devices support only one method. Base the order in which you specify methods on the ability of the remote device to correctly negotiate the appropriate method and on the level of data-line security you require. PAP usernames and passwords are sent as clear text strings, which can be intercepted and reused.

Caution If you use a *list-name* value that was not configured with the **aaa authentication ppp** command, you will disable PPP on this interface.

Table 54 lists the protocols used to negotiate PPP authentication.

Table 54 ppp authentication Protocols

chap	Enables CHAP on a serial interface.
eap	Enables EAP on a serial interface.
ms-chap	Enables MS-CHAP on a serial interface.
pap	Enables PAP on a serial interface.

Enabling or disabling PPP authentication does not affect the ability of the local router to authenticate itself to the remote device.

If you are using autoselect on a tty line, you can use the **ppp authentication** command to turn on PPP authentication for the corresponding interface.

MS-CHAP is the Microsoft version of CHAP. Like the standard version of CHAP, MS-CHAP is used for PPP authentication; authentication occurs between a personal computer using Microsoft Windows NT or Microsoft Windows 95 and a Cisco router or access server acting as a network access server.

To configure Cisco PDSN in compliance with the TIA/EIA/IS-835-B standard, you must configure the PDSN virtual template as follows:

```
ppp authentication chap pap optional
```

Examples

The following example configures virtual-template interface 4:

```
interface virtual-template 4
 ip unnumbered loopback0
 ppp authentication chap pap optional
```

The following example enables CHAP on asynchronous interface 4 and uses the authentication list MIS-access:

```
interface async 4
 encapsulation ppp
 ppp authentication chap MIS-access
```

The following example enables EAP on dialer interface 1:

```
interface dialer 1
 encapsulation ppp
 ppp authentication eap
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa new-model	Enables the AAA access control model.
autoselect	Configures a line to start an ARAP, PPP, or SLIP session.
encapsulation	Sets the encapsulation method used by the interface.
ppp accm	Identifies the ACCM table.
username	Establishes a username-based authentication system, such as PPP, CHAP, and PAP.

ppp authentication ms-chap-v2

To enable Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) authentication on a network access server (NAS), use the **ppp authentication ms-chap-v2** command in interface configuration mode. To disable MSCHAP V2 authentication, use the **no** form of this command.

ppp authentication ms-chap-v2

no ppp authentication ms-chap-v2

Syntax Description

This command has no arguments or keywords.

Command Default

MSCHAP V2 authentication is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To enable MSCHAP V2 authentication, first configure PPP on the NAS. For the NAS to properly interpret authentication failure attributes and vendor-specific attributes, the **ppp max-bad-auth** command must be configured to allow at least two authentication retries and the **radius-server vsa send** command and **authentication** keyword must be enabled. The NAS must be able to interpret authentication failure attributes and vendor-specific attributes to support the ability to change an expired password.

Examples

The following example configures PPP on an asynchronous interface and enables MSCHAP V2 authentication locally:

```
interface Async65
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
 async mode dedicated
 no peer default ip address
 ppp max-bad-auth 3
 ppp authentication ms-chap-v2
 username client password secret
```

The following example configures PPP on an asynchronous interface and enables MSCHAP V2 authentication via RADIUS:

```
interface Async65
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
 async mode dedicated
 no peer default ip address
 ppp max-bad-auth 3
 ppp authentication ms-chap-v2
 exit
aaa authentication ppp default group radius
 radius-server host 10.0.0.2 255.0.0.0
 radius-server key secret
 radius-server vsa send authentication
```

Related Commands

Command	Description
debug aaa authentication	Displays information on AAA/TACACS+ authorization.
debug ppp	Displays information on traffic and exchanges in a network that is implementing PPP.
debug radius	Displays information associated with RADIUS.
ppp max-bad-auth	Configures a point-to-point interface not to reset itself immediately after an authentication failure but instead to allow a specified number of authentication retries.
radius-server vsa send	Configures the network access server to recognize and use VSAs.

ppp authorization

To enable authentication, authorization, and accounting (AAA) authorization on the selected interface, use the **ppp authorization** command in interface configuration mode. To disable authorization, use the **no** form of this command.

ppp authorization [**default** | *list-name*]

no ppp authorization

Syntax Description

default	(Optional) The name of the method list is created with the **aaa authorization** command.
list-name	(Optional) Specifies the name of a list of authorization methods to use. If no list name is specified, the system uses the default. The list is created with the **aaa authorization** command.

Defaults

Authorization is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

After you enable the **aaa authorization** command and define a named authorization method list (or use the default method list), you must apply the defined lists to the appropriate interfaces for authorization to take place. Use the **ppp authorization** command to apply the specified method lists (or if none is specified, the default method list) to the selected interface.

Examples

The following example enables authorization on asynchronous interface 4 and uses the method list named charlie:

```
interface async 4
 encapsulation ppp
 ppp authorization charlie
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.

ppp chap hostname

To create a pool of dialup routers that all appear to be the same host when authenticating with Challenge Handshake Authentication Protocol (CHAP), use the **ppp chap hostname** command in interface configuration mode. To disable this function, use the **no** form of this command.

ppp chap hostname *hostname*

no ppp chap hostname *hostname*

Syntax Description

hostname	The name sent in the CHAP challenge.

Defaults

Disabled. The router name is sent in any CHAP challenges.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **ppp chap hostname** command allows you to specify a common alias for all routers in a rotary group to use so that only one username must be configured on the dialing routers.

This command is normally used with local CHAP authentication (when the router authenticates to the peer), but it can also be used for remote CHAP authentication.

Note By default, after changing hostnames, an MLP member link does not undergo failure recovery automatically. You must use the **ppp chap hostname** command to define the Multilink PPP (MLP) bundle name on an endpoint. If this command is not configured and the hostname is changed, then a link flap will not return the link back to the bundle.

Examples

The following example shows how to identify dialer interface 0 as the dialer rotary group leader and specify ppp as the encapsulation method used by all member interfaces. This example shows that CHAP authentication is used on received calls only and the username ISPCorp will be sent in all CHAP challenges and responses.

```
interface dialer 0
 encapsulation ppp
 ppp authentication chap callin
 ppp chap hostname ISPCorp
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp chap password	Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer.
ppp chap refuse	Refuses CHAP authentication from peers requesting it.
ppp chap wait	Specifies that the router will not authenticate to a peer requesting CHAP authentication until after the peer has authenticated itself to the router.

ppp chap password

To enable a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common Challenge Handshake Authentication Protocol (CHAP) secret password to use in response to challenges from an unknown peer, use the **ppp chap password** command in interface configuration mode. To disable the PPP CHAP password, use the **no** form of this command.

ppp chap password *secret*

no ppp chap password *secret*

Syntax Description

secret	The secret used to compute the response value for any CHAP challenge from an unknown peer.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command allows you to replace several username and password configuration commands with a single copy of this command on any dialer interface or asynchronous group interface.

This command is used for remote CHAP authentication only (when routers authenticate to the peer) and does not affect local CHAP authentication.

Examples

The commands in the following example specify ISDN BRI number 0. The method of encapsulation on the interface is PPP. If a CHAP challenge is received from a peer whose name is not found in the global list of usernames, the encrypted secret 7 1267234591 is decrypted and used to create a CHAP response value.

```
interface bri 0
 encapsulation ppp
 ppp chap password 7 1234567891
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp authentication ms-chap-v2	Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP.
ppp chap refuse	Refuses CHAP authentication from peers requesting it.
ppp chap wait	Specifies that the router will not authenticate to a peer requesting CHAP authentication until after the peer has authenticated itself to the router.

ppp chap refuse

To refuse Challenge Handshake Authentication Protocol (CHAP) authentication from peers requesting it, use the **ppp chap refuse** command in interface configuration mode. To allow CHAP authentication, use the **no** form of this command.

ppp chap refuse [**callin**]

no ppp chap refuse [**callin**]

Syntax Description

callin	(Optional) This keyword specifies that the router will refuse to answer CHAP authentication challenges received from the peer, but will still require the peer to answer any CHAP challenges the router sends.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command specifies that CHAP authentication is disabled for all calls, meaning that all attempts by the peer to force the user to authenticate using CHAP will be refused. If the **callin** keyword is used, CHAP authentication is disabled for incoming calls from the peer, but will still be performed on outgoing calls to the peer.

If outbound Password Authentication Protocol (PAP) has been enabled (using the **ppp pap sent-username** command), PAP will be suggested as the authentication method in the refusal packet.

Examples

The following example specifies ISDN BRI number 0. The method of encapsulation on the interface is PPP. This example disables CHAP authentication from occurring if a peer calls in requesting CHAP authentication.

```
interface bri 0
 encapsulation ppp
 ppp chap refuse
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp authentication ms-chap-v2	Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP.
ppp chap password	Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer.
ppp chap wait	Specifies that the router will not authenticate to a peer requesting CHAP authentication until after the peer has authenticated itself to the router.

ppp chap wait

To specify that the router will not authenticate to a peer requesting Challenge Handshake Authentication Protocol (CHAP) authentication until after the peer has authenticated itself to the router, use the **ppp chap wait** command in interface configuration mode. To allow the router to respond immediately to an authentication challenge, use the **no** form of this command.

ppp chap wait *secret*

no ppp chap wait *secret*

Syntax Description

secret	The secret used to compute the response value for any CHAP challenge from an unknown peer.

Defaults

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command (which is enabled by default) specifies that the router will not authenticate to a peer requesting CHAP authentication until the peer has authenticated itself to the router. The **no** form of this command specifies that the router will respond immediately to an authentication challenge.

Examples

The following example specifies ISDN BRI number 0. The method of encapsulation on the interface is PPP. This example disables the default, meaning that users do not have to wait for peers to complete CHAP authentication before authenticating themselves.

```
interface bri 0
 encapsulation ppp
 no ppp chap wait
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp authentication ms-chap-v2	Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP.
ppp chap password	Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer.
ppp chap refuse	Refuses CHAP authentication from peers requesting it.

ppp eap identity

To specify the Extensible Authentication Protocol (EAP) identity, use the **ppp eap identity** command in interface configuration mode. To remove the EAP identity from your configuration, use the **no** form of this command.

ppp eap identity *string*

no ppp eap identity *string*

Syntax Description

string	EAP identity.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.\
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ppp eap identity** command to configure the client to use a different identity when requested by the peer.

Examples

The following example shows how to enable EAP on dialer interface 1 and set the identity to “cat”:

```
interface dialer 1
 encapsulation ppp
 ppp eap identity cat
```

ppp eap local

To authenticate locally instead of using the RADIUS back-end server, use the **ppp eap local** command in interface configuration mode. To reenable proxy mode (which is the default), use the **no** form of this command.

ppp eap local

no ppp eap local

Syntax Description

This command has no arguments or keywords.

Defaults

Authentication is performed via proxy mode.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

By default, Extensible Authentication Protocol (EAP) runs in proxy mode. This means that EAP allows the entire authentication process to be negotiated by the network access server (NAS) to a back-end server that may reside on or be accessed via a RADIUS server. To disable proxy mode (and thus to authenticate locally instead of via RADIUS), use the **ppp eap local** command.

In local mode, the EAP session is authenticated using the MD5 algorithm and obeys the same authentication rules as does Challenge Handshake Authentication Protocol (CHAP).

Examples

The following example shows how to configure EAP to authenticate locally:

```
interface dialer 1
 encapsulation ppp
 ppp authentication eap
 ppp eap local
```

Related Commands

Command	Description
ppp authentication	Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.

ppp eap password

To set the Enhanced Authentication Protocol (EAP) password for peer authentication, use the **ppp eap password** command in interface configuration mode. To disable the password, use the **no** form of this command.

ppp eap password [*number*] *string*

no ppp eap password [*number*] *string*

Syntax Description

number	(Optional) Encryption type, including values 0 through 7; 0 means no encryption.
string	Character string that specifies the EAP password.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

For remote EAP authentication only, you can configure your router to create a common EAP password to use in response to challenges from an unknown peer; for example, if your router calls a rotary of routers (either from another vendor or from an older running version of the Cisco IOS software) to which a new (that is, unknown) router has been added, the common password will be used to respond to the new router. The **ppp eap password** command allows you to replace several username and password configuration commands with a single copy of this command on any dialer interface or asynchronous group interface.

Examples

The following example shows how to set the EAP password “7 141B1309” on the client:

```
ppp eap identity user
ppp eap password 7 141B1309
```

ppp eap refuse

To refuse Enhanced Authentication Protocol (EAP) from peers requesting it, use the **ppp eap refuse** command in interface configuration mode. To return to the default, use the **no** form of this command.

ppp eap refuse [**callin**]

no ppp eap refuse [**callin**]

Syntax Description

callin	(Optional) Authentication is refused for incoming calls only.

Defaults

The server will not refuse EAP authentication challenges received from the peer.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ppp eap refuse** command to disable EAP authentication for all calls. If the **callin** keyword is used, the server will refuse to answer EAP authentication challenges received from the peer but will still require the peer to answer any EAP challenges the server sends.

Examples

The following example shows how to refuse EAP authentication on incoming calls from the peer:

```
ppp authentication eap
ppp eap local
ppp eap refuse callin
```

Related Commands

Command	Description
ppp authentication	Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.

ppp eap wait

To configure the server to delay the Enhanced Authentication Protocol (EAP) authentication until after the peer has authenticated itself to the server, use the **ppp eap wait** command in interface configuration mode. To disable this functionality, use the **no** form of this command.

ppp eap wait

no ppp eap wait

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ppp eap wait** command to specify that the server will not authenticate to a peer requesting EAP authentication until after the peer has authenticated itself to the server.

Examples

The following example shows how to configure the server to wait for the peer to authenticate itself first:

```
ppp authentication eap
ppp eap local
ppp eap wait
```

Related Commands

Command	Description
ppp authentication	Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.

ppp link

To generate the Point-to-Point Protocol (PPP) Link Control Protocol (LCP) down and keepalive-failure link traps or enable calls to the interface-reset vector, use the **ppp link** command in interface configuration mode. To disable the PPP LCP down and keepalive-failure link traps or calls to the interface-reset vector, use the **no** form of this command.

ppp link {**reset** | **trap**}

no ppp link {**reset** | **trap**}

Syntax Description

reset	Specifies calls to the interface reset vector.
trap	Specifies the PPP LCP down and keepalive-failure link traps.

Defaults

The defaults are as follows:

- The calls are sent to the interface-reset vector.
- The traps are sent when the LCP goes down.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

The **no ppp link trap** command disables the sending of the link traps when the LCP goes down.

In the event that the PPP calls the interface-reset vector while the LCP is configured or closed, Up/Down status messages will display on the console. If a leased-line configuration is up but the peer is not responding, PPP may call the interface-reset vector once per minute. This situation may result in the Up/Down status messages on the console. Use the **no ppp link reset** command to disable calls to the interface-reset vector. PPP will continue to attempt to negotiate with the peer, but the interface will not be reset between each attempt.

Examples

This example shows how to enable calls to the interface-reset vector:

```
Router(config-if)# ppp link reset
Router(config-if)#
```

This example shows how to disable calls to the interface-reset vector:

```
Router(config-if)# no ppp link reset
Router(config-if)#
```

This example shows how to generate the PPP LCP down/keepalive-failure link traps:

```
Router(config-if)# ppp link trap
Router(config-if)#
```

This example shows how to disable the sending of the link traps when the LCP goes down:

```
Router(config-if)# no ppp link trap
Router(config-if)#
```

ppp pap refuse

To refuse a peer request to authenticate remotely with PPP using Password Authentication Protocol (PAP), use the **ppp pap refuse** command in interface configuration mode. To disable the refusal, use the **no** form of this command.

ppp pap refuse

no ppp pap refuse

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to refuse remote PAP support; for example, to respond to the peer request to authenticate with PAP.

This is a per-interface command.

Examples

The following example shows how to enable the **ppp pap** command to refuse a peer request for remote authentication:

```
interface dialer 0
 encapsulation ppp
 ppp pap refuse
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP and TACACS+.
encapsulation ppp	Sets PPP as the encapsulation method used by a serial or ISDN interface.

Command	Description
ppp authentication	Enables CHAP or PAP or both, and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp pap sent-username	Reenables remote PAP support for an interface and uses the **sent-username** and **password** in the PAP authentication request packet to the peer.

ppp pap sent-username

To reenable remote Password Authentication Protocol (PAP) support for an interface and use the **sent-username** and **password** in the PAP authentication request packet to the peer, use the **ppp pap sent-username** command in interface configuration mode. To disable remote PAP support, use the **no** form of this command.

ppp pap sent-username *username* **password** *password*

no ppp pap sent-username

Syntax Description

username	Username sent in the PAP authentication request.
password	Password sent in the PAP authentication request.
password	Must contain from 1 to 25 uppercase and lowercase alphanumeric characters.

Defaults

Remote PAP support disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to reenable remote PAP support (for example, to respond to the peer's request to authenticate with PAP) and to specify the parameters to be used when sending the PAP authentication request.

This is a per-interface command. You must configure this command for each interface.

Examples

The following example identifies dialer interface 0 as the dialer rotary group leader and specify PPP as the method of encapsulation used by the interface. Authentication is by CHAP or PAP on received calls only. *ISPCorp* is the username sent to the peer if the peer requires the router to authenticate with PAP.

```
interface dialer0
 encapsulation ppp
 ppp authentication chap pap callin
 ppp chap hostname ISPCorp
 ppp pap sent username ISPCorp password 7 fjhfeu
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp authentication ms-chap-v2	Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP.
ppp chap password	Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer.

preempt

To enable preemption on the redundancy group, use the **preempt** command in redundancy application group configuration mode**.** To disable the group's preemption, use the **no** form of this command.

preempt

no preempt

Syntax Description

This command has no arguments or keywords.

Command Default

Preemption is disabled on the redundancy group.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

When the preemption is enabled, it means that a standby redundancy group should preempt an active redundancy group if its priority is higher than the active redundancy group.

Examples

The following example shows how to enable preemption on the redundancy group:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp) preempt
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
protocol	Defines a protocol instance in a redundancy group.

pre-shared-key

To define a preshared key to be used for Internet Key Exchange (IKE) authentication, use the **pre-shared-key** command in keyring configuration mode. To disable the preshared key, use the **no** form of this command.

pre-shared-key {**address** *address* [*mask*] | **hostname** *hostname* | **ipv6** {*ipv6-address* | *ipv6-prefix*}} **key** *key*

no pre-shared-key {**address** *address* [*mask*] | **hostname** *hostname* | **ipv6** {*ipv6-address* | *ipv6-prefix*}} **key** *key*

Syntax Description

address *address* [*mask*]	IP address of the remote peer or a subnet and mask. The *mask* argument is optional.
hostname *hostname*	Fully qualified domain name (FQDN) of the peer.
ipv6	Specifies that an IPv6 address of a remote peer will be used.
ipv6-address	IPv6 address of the remote peer. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
ipv6-prefix	IPv6 prefix of the remote peer.
key *key*	Specifies the secret.

Command Default

None

Command Modes

Keyring configuration (config-keyring)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(2)T	This command was modified so that output for the **pre-shared-key** command will show that the preshared key is either encrypted or unencrypted.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(4)T	The **ipv6** keyword and the *ipv6-address* and *ipv6-prefix* arguments were added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Before configuring preshared keys, you must configure an Internet Security Association and Key Management Protocol (ISAKMP) profile.

Output for the **pre-shared-key** command will show that the preshared key is either unencrypted or encrypted. An output example for an unencrypted preshared key would be as follows:

```
pre-shared-key address 10.1.0.1 key test123
```

An output example for a type 6 encrypted preshared key would be as follows:

```
pre-shared-key address 10.1.0.1 key 6 RHZE[JACMUI\bcbTdELISAAB
```

Examples

The following example shows how to configure a preshared key using an IP address and hostname:

```
Router(config)# crypto keyring vpnkeyring
Router(config-keyring)# pre-shared-key address 10.72.23.11 key vpnkey
Router(config-keyring)# pre-shared-key hostname www.vpn.com key vpnkey
```

Related Commands

Command	Description
crypto keyring	Defines a crypto keyring to be used during IKE authentication.

pre-shared-key (IKEv2 keyring)

To define a preshared key for an Internet Key Exchange Version 2 (IKEv2) peer, use the **pre-shared-key** command in IKEv2 keyring peer configuration mode. To disable the preshared key, use the **no** form of this command.

pre-shared-key {**local** | **remote**} {**0** | **6** | *line*}

no pre-shared-key {**local** | **remote**}

Syntax Description

0	Specifies that the password is unencrypted.
6	Specifies that the password is encrypted.
line	Specify an unencrypted user password.
local	Specifies the signing key.
remote	Specifies the verifying key.

Command Default

The default is a symmetric key.

Command Modes

IKEv2 keyring peer configuration (config-ikev2-keyring-peer)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to specify the preshared key for the peer. Use the **local** or **remote** keywords to specify an asymmetric key.

Examples

The following examples shows how to configure a preshared key in different scenarios.

IKEv2 Keyring with Symmetric Preshared Keys Based on IP Address

The following is the initiator's keyring:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# description peer1
Router(config-ikev2-keyring-peer)# address 10.0.0.1
Router(config-ikev2-keyring-peer)# pre-shared-key key-1
```

The following is the responder's keyring:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer2
Router(config-ikev2-keyring-peer)# description peer2
```

```
Router(config-ikev2-keyring-peer)# address 10.0.0.3
Router(config-ikev2-keyring-peer)# pre-shared-key key-1
```

IKEv2 Keyring with Asymmetric Preshared Keys Based on IP Address

The following is the initiator's keyring:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# description peer1 with asymmetric keys
Router(config-ikev2-keyring-peer)# address 10.0.0.1
Router(config-ikev2-keyring-peer)# pre-shared-key local key-1
Router(config-ikev2-keyring-peer)# pre-shared-key remote key-2
```

The following is the responder's keyring:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer2
Router(config-ikev2-keyring-peer)# description peer2 with asymmetric keys
Router(config-ikev2-keyring-peer)# address 10.0.0.3
Router(config-ikev2-keyring-peer)# pre-shared-key local key-2
Router(config-ikev2-keyring-peer)# pre-shared-key remote key-1
```

IKEv2 Keyring with Asymmetric Preshared Key Based on Hostname

The following is the initiator's keyring:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer host1
Router(config-ikev2-keyring-peer)# description host1 in abc domain
Router(config-ikev2-keyring-peer)# host host1.example.com
Router(config-ikev2-keyring-peer)# pre-shared-key local key-1
Router(config-ikev2-keyring-peer)# pre-shared-key remote key-2
```

The following is the responder's keyring:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer host2
Router(config-ikev2-keyring-peer)# description host2 in example domain
Router(config-ikev2-keyring-peer)# host host2.example.com
Router(config-ikev2-keyring-peer)# pre-shared-key local key-2
Router(config-ikev2-keyring-peer)# pre-shared-key remote key-1
```

IKEv2 Keyring with Symmetric Preshared Key Based on Identity

```
Router(config)# crypto ikev2 keyring keyring-4
Router(config-ikev2-keyring)# peer abc
Router(config-ikev2-keyring-peer)# description example domain
Router(config-ikev2-keyring-peer)# identity fqdn example.com
Router(config-ikev2-keyring-peer)# pre-shared-key abc-key-1

Router(config-ikev2-keyring)# peer user1
Router(config-ikev2-keyring-peer)# description user1 in example domain
Router(config-ikev2-keyring-peer)# identity email user1@example.com
Router(config-ikev2-keyring-peer)# pre-shared-key abc-key-2

Router(config)# peer user1-remote
Router(config-ikev2-keyring)# description user1 abc remote users
Router(config-ikev2-keyring-peer)# identity key-id abc
Router(config-ikev2-keyring-peer)# pre-shared-key abc-key-3
```

IKEv2 Keyring with a Wildcard Key

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# description ABCdomain
```

```
Router(config-ikev2-keyring-peer)# address 0.0.0.0 0.0.0.0
Router(config-ikev2-keyring-peer)# pre-shared-key abc-key
```

Related Commands

Command	Description
crypto ikev2 keyring	Defines an IKEv2 keyring.
description (ikev2 keying)	Describes an IKEv2 peer or a peer group for the IKEv2 keyring.
hostname (ikev2 keyring)	Specifies the hostname for the peer in the IKEv2 keyring.
peer	Defines a peer or a peer group for the keyring.
address (ikev2 keyring)	Specifies the IPv4 address or the range of the peers in IKEv2 keyring.
identity (ikev2 keyring)	Identifies the peer with IKEv2 types of identity.

primary

To assign a specified trustpoint as the primary trustpoint of the router, use the **primary** command in ca-trustpoint configuration mode.

primary *name*

Syntax Description

name	Name of the primary trustpoint of the router.

Defaults

No default behavior or values.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

Use the **primary** command to specify a given trustpoint as primary.

Before you can configure this command, you must enable the **crypto ca trustpoint** command, which defines the trustpoint and enters ca-trustpoint configuration mode.

Examples

The following example shows how to configure the trustpoint “ka” as the primary trustpoint:

```
crypto ca trustpoint ka
 enrollment url http://xxx
 primary
 crl optional
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

priority(firewall)

To specify a group priority and failover threshold value in a redundancy group, use the **priority** command in redundancy application group configuration mode**.** To disable the priority value of a group, use the **no** form of this command.

priority *value* [**failover-threshold** *value*]

no priority *value* [**failover-threshold** *value*]

Syntax Description

value	The priority value. The range is from 1 to 255.
failover-threshold *value*	(Optional) Specifies the failover threshold value. The range is from 1 to 255.

Command Default

The default priority value is 100.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The priority of the redundancy group is used to determine a redundancy group's active or standby role on the configured node. The failover threshold is used to determine when a switchover must occur. After the priority is set under threshold, the active redundancy group gives up its role.

Examples

The following example shows how to configure the priority value and threshold value for the redundancy group named group1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp) priority 100 failover-threshold 90
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.

private-hosts

To globally enable the Private Hosts feature, use the **private-hosts** command in global configuration mode. To disable the feature, use the **no** form of this command.

private-hosts

no private-hosts

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into the Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Issue this command to enable the Private Hosts feature on the router. Then, use the **private-hosts mode** command to enable Private Hosts on individual interfaces (ports).

Examples

The following example globally enables the Private Hosts feature on the router:

```
Router(config)# private-hosts
```

Related Commands

Command	Description
private-hosts mac list	Creates a MAC address list that identifies the content servers providing broadband services to isolated hosts.
private-hosts mode	Specifies the operating mode for a Private Hosts port.
private-hosts promiscuous	Identifies the content servers and receiving hosts for broadband services.
private-hosts vlan-list	Identifies the VLANs whose hosts need to be isolated.
show private-hosts configuration	Displays Private Hosts configuration information for the router.
show private-hosts interface configuration	Displays Private Hosts configuration information for individual interfaces.

private-hosts layer3

To globally enable Layer 3 routing on private hosts, use the **private-hosts layer3** command in global configuration mode. To disable the feature, use the **no** form of this command.

private-hosts layer3

no private-hosts layer3

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRD	This command was introduced.

Usage Guidelines

Use this command to enable the private hosts layer 3 routing on the router.

Examples

The following example shows the layer 3 configuration enabled on private hosts:

```
Router(config)# private-hosts layer3

Router# show private-hosts configuration
Private hosts disabled. BR INDEX 65536
Layer-3 switching on Private Hosts is enabled
Missing config: MAC list, VLAN list, MAC list association, Enable command, Atlea
st one Promiscuous/Mixed port
Privated hosts vlans lists:
None
```

Related Commands

Command	Description
private-hosts mac list	Creates a MAC address list that identifies the content servers providing broadband services to isolated hosts.
private-hosts promiscuous	Identifies the content servers and receiving hosts for broadband services.
private-hosts vlan-list	Identifies the VLANs whose hosts need to be isolated.
show private-hosts configuration	Displays Private Hosts configuration information for the router.

private-hosts mac-list

To identify the content servers that provide broadband services to isolated hosts, create a MAC address list by using the **private-hosts mac-list** command in global configuration mode. To delete an address from the MAC address list and remove that device from the list of content servers providing services for the Private Hosts feature, use the **no** form of this command.

private-hosts mac-list *mac-list-name mac-address* [**remark** *device-name* | *comment*]

no private-hosts mac-list *mac-list-name mac-address*

Syntax Description

mac-list-name	A name to assign to the address list (up to 80 characters).
mac-address	The MAC address of a Broadband Remote Access Server (BRAS), multicast server, or video server that provides broadband services for the Private Hosts feature. **Note** If the server is not directly connected to the networking device, specify the MAC address of the core network device that provides access to the server.
remark *device-name* | *comment*	(Optional) Specifies an optional device name or comment to assign to this MAC address list.

Command Default

The MAC address list is not populated with content servers.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command creates a list of MAC addresses that identify the content servers being used to provide broadband services to isolated hosts in the Private Hosts configuration. The Private Hosts feature uses port-based Protocol-Independent MAC ACLs (PACLs) to provide Layer 2 isolation between hosts on trusted ports within a purely Layer 2 domain. The PACLs isolate the hosts by imposing Layer 2 forwarding constraints on the router ports.

Use this command to specify the MAC address of every content server that provides broadband services for the Private Hosts feature. A *content server* is any BRAS, multicast server, or video server that provides services to the isolated hosts in your network.

You can assign all of the content servers to a single MAC address list or you can create multiple MAC address lists, each identifying the content server for a particular type of broadband service or set of services. When you configure the promiscuous ports for Private Hosts, you specify a MAC address list and VLAN list to identify the server and receiving hosts for broadband services.

If you plan to deliver different types of broadband services to different sets of hosts, create multiple MAC address lists to identify the servers for each type of service. You can also create multiple VLAN lists to identify different sets of isolated hosts. When you configure promiscuous ports, you can specify different combinations of MAC address lists and VLAN lists to identify the servers and receiving hosts for each type of service.

Note The MAC address list is deleted when the last address in the list is deleted.

Examples

This example creates a MAC address list named BRAS1 that identifies the MAC address of the upstream BRAS. The optional remark names the MAC address list BRAS1.

```
Router(config)# private-hosts mac-list BRAS1 0000.1111.1111 remark BRAS1
```

Related Commands

Command	Description
show private-hosts mac-list	Displays a list of the MAC addresses that identify the content servers that are providing broadband defined for Private Hosts.

private-hosts mode

To enable Private Hosts on an interface (port) and specify the mode in which the port is to operate, use the **private-hosts mode** command in interface configuration mode. To disable Private Hosts on the port, use the **no** form of this command.

private-hosts mode {**promiscuous** | **isolated** | **mixed**}

no private-hosts

Syntax Description

promiscuous	Configures the port for promiscuous mode. Use this mode for ports that face upstream. These are the ports that connect the router to the servers providing broadband services (Broadband Remote Access Server [BRAS], multicast, or video), or to the core network devices providing access to the servers.
isolated	Configures the port for isolated mode. Use this mode for ports that face the DSL access multiplexer (DSLAM) to which the isolated hosts are connected.
mixed	Configures the port for mixed mode. Use this mode for ports that connect to other networking devices, typically in a ring topology. The behavior of this port can change depending on the Spanning Tree Protocol (STP) topology.

Command Modes

This command is disabled by default.
The default for the **mode** keyword is promiscuous.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Before you can use this command, you must globally enable the Private Hosts feature on the router by issuing the **private-hosts** command.

Use this command to enable the Private Hosts feature on individual ports and to define the mode of operation for the port. A port's mode determines which type of Protocol-Independent MAC ACLs (PACL) will be assigned to the port in order to restrict the type of traffic that is allowed to pass through the port. Each type of PACL restricts the traffic flow for a different type of traffic (for example, from content servers to isolated hosts, from isolated hosts to servers, and traffic between isolated hosts). Use the **show private-hosts interface configuration** command to display the mode assigned to Private Hosts ports.

Examples

The following command example enables Private Hosts on an interface (port) and configures the port for isolated mode:

```
Router(config-if)# private-hosts mode isolated
```

Related Commands

Command	Description
private-hosts	Enables or configures the private hosts feature.
show fm private-hosts	Displays the FM-related private hosts information.
show private-hosts	Displays the private hosts information.
show private-hosts interface configuration	Displays Private Hosts configuration information for individual interfaces.

private-hosts promiscuous

To identify the content servers and receiving hosts for broadband services, use the **private-hosts promiscuous** command in global configuration mode. To remove a promiscuous ports setting, use the **no** form of this command.

private-hosts promiscuous *mac-list-name* [**vlan** *vlan-ids*]

no private-hosts promiscuous *mac-list-name*

Syntax Description

mac-list-name	The name of MAC address list that identifies the content servers (Broadband Remote Access Server [BRAS], multicast, or video) providing broadband services for the Private Hosts feature.
vlan *vlan-ids*	(Optional) The VLAN or set of VLANs whose hosts will be allowed to receive services from the content servers identified by the MAC address list. Use commas to separate individual VLANs and hyphens to specify a range of VLANs (for example, 1,3,5,20-25). **Note** If no VLAN list is specified, the global VLAN list is used.

Defaults

Promiscuous ports are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The MAC address list and VLAN list define the content servers and receiving hosts for broadband services. If no VLAN list is specified, the system uses the global VLAN list created with the **private-hosts vlan-list** command.

You can issue this command multiple times to specify multiple combinations of MAC and VLAN lists, each defining the server and receiving hosts for a particular type of service. For example, the BRAS at xxxx.xxxx.xxxx could be used to deliver a basic set of services over VLANs 20, 25, and 30, and the BRAS at yyyy.yyyy.yyyy could be used to deliver a premium set of services over VLANs 5, 10, and 15.

Examples

The following example configures the broadband services provided by the content servers defined in the BRASlist address list to be delivered to the isolated hosts in VLANs 10, 12, 15, and 200 through 300:

```
Router(config)# private-hosts promiscuous BRASlist vlan 10,12,15,200-300
```

Related Commands

Command	Description
private-hosts vlan-list	Creates a VLAN list to be used to identify the VLANs whose hosts need to be isolated from each other (so that the VLANs can be used to deliver broadband services).
show private-hosts configuration	Displays Private Hosts configuration information for the router.
show private-hosts interface configuration	Displays Private Hosts configuration information for individual interfaces.

private-hosts vlan-list

To create a VLAN list to be used to identify the VLANs whose hosts need to be isolated from each other (so that the VLANs can be used to deliver broadband services) use the **private-hosts vlan-list** command in global configuration mode. To remove a VLAN from the list of VLANs requiring host isolation, use the **no** form of this command.

private-hosts vlan-list *vlan-ids*

no private-hosts vlan-list *vlan-ids*

Syntax Description

vlan-ids	A list of the VLANs whose hosts need to be isolated from each other. Use commas to separate individual VLANs and hyphens to specify a range of VLANs (for example, 1,3,5,20-25).

Command Default

A VLAN is not included in the list of VLANs requiring host isolation.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command creates a list of VLANs whose hosts need to be isolated through the Private Hosts feature. The VLAN list should include all of the VLANs that are being used to deliver broadband services to multiple end users (isolated hosts).

If you plan to deliver different types of broadband services to different sets of hosts, you can create multiple VLAN lists and multiple MAC address lists. When you configure promiscuous ports, you can specify different combinations of MAC and VLAN lists to identify the content servers and receiving hosts for each type of service.

If you do not specify a VLAN list when you configure promiscuous ports, the system uses the global VLAN list created by this command.

Note The Private Hosts feature isolates the hosts in all of the VLANs included in VLAN lists; therefore, VLAN lists should include only those VLANs that are being used to deliver broadband services.

Examples

This example shows how to configure the Private Hosts feature to isolate the hosts in VLANs 10, 12, 15, and 200 through 300:

```
Router(config)# private-hosts vlan-list 10,12,15,200-300
```

Related Commands

Command	Description
show private-hosts configuration	Displays Private Hosts configuration information for the router.

privilege

To configure a new privilege level for users and associate commands with that privilege level, use the **privilege** command in global configuration mode. To reset the privilege level of the specified command or commands to the default and remove the privilege level configuration from the running configuration file, use the **no** form of this command.

Note As of Cisco IOS Releases 12.3(6) and 12.3(6)T, the **no** form of the **privilege** command and the **reset** keyword perform the same functions.

privilege *mode* [**all**] {**level** *level* | **reset**} *command-string*

no privilege *mode* [**all**] {**level** *level* | **reset**} *command-string*

Syntax Description

mode	Configuration mode for the specified command. See Table 55 in the "Usage Guidelines" section for a list of options for this argument.
all	(Optional) Changes the privilege level for all the suboptions to the same level.
level *level*	Specifies the privilege level you are configuring for the specified command or commands. The level argument must be a number from 0 to 15.
reset	Resets the privilege level of the specified command or commands to the default and removes the privilege level configuration from the running configuration file. **Note** For Cisco IOS software releases earlier than Release 12.3(6) and Release 12.3(6)T, you use the **no** form of this command to reset the privilege level to the default. The default form of this command will still appear in the configuration file. To completely remove a privilege configuration, use the **reset** keyword.
command-string	Command associated with the specified privilege level. If the **all** keyword is used, specifies the command and subcommands associated with the privilege level.

Defaults

User EXEC mode commands are privilege level 1.

Privileged EXEC mode and configuration mode commands are privilege level 15.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(22)S, 12.2(13)T	The **all** keyword was added.
12.3(6), 12.3(6)T	The **no** form of the command performs the same function as the **reset** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The password for a privilege level defined using the **privilege** global configuration command is configured using the **enable secret** command.

Level 0 can be used to specify a more-limited subset of commands for specific users or lines. For example, you can allow user "guest" to use only the **show users** and **exit** commands.

Note There are five commands associated with privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. If you configure AAA authorization for a privilege level greater than 0, these five commands will not be included.

When you set the privilege level for a command with multiple words, note that the commands starting with the first word will also have the specified access level. For example, if you set the **show ip route** command to level 15, the **show** commands and **show ip** commands are automatically set to privilege level 15—unless you set them individually to different levels. This is necessary because you can't execute, for example, the **show ip** command unless you have access to **show** commands.

To change the privilege level of a group of commands, use the **all** keyword. When you set a group of commands to a privilege level using the **all** keyword, all commands which match the beginning string are enabled for that level, and all commands which are available in submodes of that command are enabled for that level. For example, if you set the **show ip** keywords to level 5, show and ip will be changed to level 5 and all the options that follow the **show ip** string (such as **show ip accounting**, **show ip aliases**, **show ip bgp**, and so on) will be available at privilege level 5.

Table 55 shows some of the keyword options for the mode argument in the **privilege** command. The available mode keywords will vary depending on your hardware and software version. To see a list of available mode options on your system, use the **privilege ?** command.

Table 55 mode Argument Options

Command	Description
accept-dialin	VPDN group accept dialin configuration mode
accept-dialout	VPDN group accept dialout configuration mode
address-family	Address Family configuration mode
alps-ascu	ALPS ASCU configuration mode
alps-circuit	ALPS circuit configuration mode
atm-bm-config	ATM bundle member configuration mode
atm-bundle-config	ATM bundle configuration mode

Table 55 mode Argument Options (continued)

Command	Description
atm-vc-config	ATM virtual circuit configuration mode
atmsig_e164_table_mode	ATMSIG E164 Table
cascustom	Channel-associated signalling (cas) custom configuration mode
config-rtr-http	RTR HTTP raw request Configuration
configure	Global configuration mode
controller	Controller configuration mode
crypto-map	Crypto map config mode
crypto-transform	Crypto transform config modeCrypto transform configuration mode
dhcp	DHCP pool configuration mode
dspfarm	DSP farm configuration mode
exec	Exec mode
flow-cache	Flow aggregation cache configuration mode
gateway	Gateway configuration mode
interface	Interface configuration mode
interface-dlci	Frame Relay DLCI configuration mode
ipenacl	IP named extended access-list configuration mode
ipsnacl	IP named simple access-list configuration mode
ip-vrf	Configure IP VRF parameters
lane	ATM Lan Emulation Lecs Configuration Table
line	Line configuration mode
map-class	Map class configuration mode
map-list	Map list configuration mode
mpoa-client	MPOA Client
mpoa-server	MPOA Server
null-interface	Null interface configuration mode
preaut	AAA Preauth definitions
request-dialin	VPDN group request dialin configuration mode
request-dialout	VPDN group request dialout configuration mode
route-map	Route map configuration mode
router	Router configuration mode
rsvp_policy_local	
rtr	RTR Entry Configuration
sg-radius	RADIUS server group definition
sg-tacacs+	TACACS+ server group
sip-ua	SIP UA configuration mode

Table 55 mode Argument Options (continued)

Command	Description
subscriber-policy	Subscriber policy configuration mode
tcl	Tcl mode
tdm-conn	TDM connection configuration mode
template	Template configuration mode
translation-rule	Translation Rule configuration mode
vc-class	VC class configuration mode
voiceclass	Voice Class configuration mode
voiceport	Voice configuration mode
voipdialpeer	Dial Peer configuration mode
vpdn-group	VPDN group configuration mode

Examples

The following example shows how to set the **configure** command to privilege level 14 and establish SecretPswd14 as the password users must enter to use level 14 commands:

```
privilege exec level 14 configure
enable secret level 14 SecretPswd14
```

The following example shows how to set the **show** and **ip** keywords to level 5. The suboptions coming under **ip** will also be allowed to users with privilege level 5 access:

```
Router(config)# privilege exec all level 5 show ip
```

The following two examples demonstate the difference in behavior between the **no** form of the command and the use of the **reset** keyword when using Cisco IOS software releases earlier than Releases 12.3(6) and Release 12.3(6)T.

Note As of Cisco IOS Releases 12.3(6) and 12.3(6)T, the **no** form of the **privilege** command and the **reset** keyword perform the same functions.

```
! show currently configured privilege commands
Router# show running-config | include priv
privilege configure all level 3 interface
privilege exec level 3 configure terminal
privilege exec level 3 configure

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# no privilege exec level 3 configure terminal
Router(config)# end
! show currently configured privilege commands
Router# show running-config | include priv
privilege configure all level 3 interface
privilege exec level 15 configure terminal
privilege exec level 15 configure
```

Note that in the **show running-config** output above, the privilege command for “configure terminal” still appears, but now has the default privilege level assigned.

To remove a previously configured privilege command entirely from the configuration, use the **reset** keyword, as shown in the following example:

```
! show currently configured privilege commands
Router# show running-config | include priv
privilege configure all level 3 interface
privilege exec level 3 configure terminal
privilege exec level 3 configure

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# privilege exec reset configure terminal
Router(config)#
Router# show running-config | include priv
privilege configure all level 3 interface
Router#
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
enable secret	Specifies an additional layer of security over the **enable password** command.
privilege level	Sets the default privilege level for a line.

privilege level

To set the default privilege level for a line, use the **privilege level** command in line configuration mode. To restore the default user privilege level to the line, use the **no** form of this command.

privilege level *level*

no privilege level

Syntax Description

level	Privilege level associated with the specified line.

Defaults

Level 15 is the level of access permitted by the enable password.

Level 1 is normal EXEC-mode user privileges.

Command Modes

Line configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Users can override the privilege level you set using this command by logging in to the line and enabling a different privilege level. They can lower the privilege level by using the **disable** command. If users know the password to a higher privilege level, they can use that password to enable the higher privilege level.

You can use level 0 to specify a subset of commands for specific users or lines. For example, you can allow user "guest" to use only the **show users** and **exit** commands.

You might specify a high level of privilege for your console line to restrict line usage.

Examples

The following example configures the auxiliary line for privilege level 5. Anyone using the auxiliary line has privilege level 5 by default:

```
line aux 0
 privilege level 5
```

The following example sets all **show ip** commands, which includes all **show** commands, to privilege level 7:

```
privilege exec level 7 show ip route
```

This is equivalent to the following command:

```
privilege exec level 7 show
```

The following example sets the **show ip route** to level 7 and the **show** and **show ip** commands to level 1:

```
privilege exec level 7 show ip route
privilege exec level 1 show ip
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.

profile (GDOI local server)

To define the IP security (IPsec) security association (SA) policy for a Group Domain of Interpretation (GDOI) group, use the **profile** command in GDOI local server configuration mode. To disable the IPsec SA policy that was defined, use the **no** form of this command.

profile {*ipsec-profile-name*}

no profile {*ipsec-profile-name*}

Syntax Description

ipsec-profile-name	Name of the IPsec profile.

Command Default

An IPsec SA policy is not defined for the GDOI group.

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following example shows that the IPsec SA policy has been defined as “group1234”:

```
profile group1234
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

profile (profile map configuration)

To define or modify an individual authentication and authorization cache profile, use the **profile** command in profile map configuration mode. To disable a cache profile, use the **no** form of this command.

profile *name* [**no-auth**]

no profile *name*

Syntax Description

name	Text string that is an exact match to an existing username.
no-auth	(Optional) Specifies that authentication is bypassed for this user.

Command Default

No profiles are defined.

Command Modes

Profile map configuration (config-profile-map)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **profile** command to define or modify an authentication and authorization cache profile. The *name* argument in this command must be an exact match to a username being queried by an authentication or authorization service request.

Using the **profile** command with the *name* argument, as opposed to using the **regexp** or **all** command, is the recommended way to cache information.

Examples

The following example defines a cache profile that includes no user authentication and is a part of the localusers cache profile group:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa cache profile localusers
Router(config-profile-map)# profile user101 no auth
```

Related Commands

Command	Description
aaa cache profile	Creates a named authentication and authorization cache profile group.
all	Specifies that all authentication and authorization requests be cached.
regexp	Creates an entry in a cache profile group that allows authentication and authorization matches based on a regular expression.

proposal

To specify the proposals in an Internet Key Exchange Version 2 (IKEv2) policy, use the **proposal** command in IKEv2 policy configuration mode. To delete the proposal from the policy, use the **no** form of this command.

proposal *name*

no proposal *name*

Syntax Description

name	Proposal name.

Command Default

The default proposal is used with the default policy.

Command Modes

IKEv2 policy configuration (config-ikev2-policy)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this option to specify the proposals to use with the policy. One proposal must be specified at least and additional proposals can be specified with one proposal for each statement. The proposals are prioritized in the order of listing.

Note The specified proposals must be defined. Use the **crypto ikev2 proposal** command to define a proposal.

Examples

The following example shows how to specify a proposal in an IKEv2 policy:

```
Router(config)# crypto ikev2 policy policy1
Router(config-ikev2-policy)# proposal proposal1
```

Related Commands

Command	Description
crypto ikev2 policy	Defines an IKEv2 policy.
crypto ikev2 proposal	Defines an IKE proposal.
match (ikev2 policy)	Matches an IKEv2 policy based on the parameters.
show crypto ikev2 policy	Displays the default or user-defined IKEv2 policy.

protection (zone)

To configure TCP synchronization (SYN) cookie protection against SYN-flood attacks, use the **protection** command in security zone configuration mode. To disable the SYN cookie protection, use the **no** form of this command.

protection *parameter-map-name*

no protection *parameter-map-name*

Syntax Description

parameter-map-name	Name of the parameter map.

Command Default

SYN cookie protection is not configured.

Command Modes

Security zone configuration (config-sec-zone)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Usage Guidelines

You must configure the **zone security** command before you can configure the **protection** command.

You can use the **protection** command to bind an inspect zone-type parameter map to a zone.

TCP SYN-flooding attacks are a type of denial-of-service (DoS) attack. Usually, TCP SYN packets are sent to a targeted end host or a range of subnet addresses behind the firewall.

Examples

The following example shows how to configure the TCP SYN cookie protection:

```
Router(config)# zone security zone1
Router(config-sec-zone)# protection zone-pmap
Router(config-sec-zone)# end
```

Related Commands

Command	Description
zone security	Creates a security zone and enters security zone configuration mode.

protocol

To define a protocol instance in a redundancy group, use the **protocol** command in redundancy application configuration mode**.** To remove the protocol instance from the redundancy group, use the **no** form of this command.

protocol *id*

no protocol *id*

Syntax Description

id	Redundancy group protocol ID. The range is from 1 to 8.

Command Default

Protocol instance is not defined in a redundancy group.

Command Modes

Redundancy application configuration (config-red-app)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

Protocol configuration is used to configure timers and authentication method for a control interface. Thus, a protocol instance is attached to the control interface.

Examples

The following example shows how to configure a protocol named protocol 1 to a redundancy group:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# protocol 1
Router(config-red-app-prtcl)#
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.
timers hellotime	Configures timers for hellotime and holdtime messages for a redundancy group.

proxy

To configure proxy parameters for an Easy VPN remote device, use the **proxy** command in ISAKMP browser proxy configuration mode. To disable the parameters, use the **no** form of this command.

proxy {*proxy-parameter*}

no {*proxy-parameter*}

Syntax Description

proxy-parameter	Proxy parameter. See Table 56 for a list of acceptable proxy parameters.

Command Default

Proxy parameters are not set.

Command Modes

ISAKMP browser proxy configuration (config-ikmp-browser-proxy)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

This command is a subcommand of the **crypto isakmp client configuration browser-proxy** command.

Table 56 lists acceptable proxy parameters.

Table 56 Proxy Parameters

Proxy Parameter	Result
auto-detect	Automatically detects proxy settings.
by-pass-local	Bypasses proxy server for local addresses.
exception-list	Semicolon- (;) delimited list of IP addresses.
none	No proxy settings.
server	Proxy server IP and port number (ip:port number).

Examples

The following example shows various browser-proxy parameter settings for a browser proxy named "bproxy.":

```
crypto isakmp client configuration browser-proxy bproxy
 proxy auto-detect

crypto isakmp client configuration browser-proxy bproxy
```

```
 proxy none

crypto isakmp client configuration browser-proxy bproxy
 proxy server 10.1.1.1:2000
 proxy exception-list 10.2.2.*,www.*org
 proxy by-pass-local
```

Related Commands

Command	Description
crypto isakmp client configuration browser-proxy	Configures browser-proxy parameters for an Easy VPN remote device.

qos-group (PVS Bundle Member)

To associate a quality of service (QoS) group or groups with a permanent virtual circuit (PVC) bundle-member, use the **qos-group** command in PVC bundle member configuration mode. To remove a QoS-group from a PVC bundle member, use the **no** form of this command.

qos-group *group number*

no qos-group *group number*

Syntax Description

group number <0-99>	Associates a QoS-group with a PVC bundle member. You can associate one QoS group, a range of QoS groups, or any combination of QoS groups and ranges of QoS groups, separated by commas, with a PVC bundle member. When a range of QoS groups is associated with a PVC bundle, only the starting and ending QoS group number need to be listed, separated by a hyphen. For example, 1-5. When multiple-non contiguous QoS groups or non-contiguous ranges of QoS groups are associated with a PVC bundle, separate the groups. For example, 1, 3, 8-10, 12-14. When a QoS group is associated with a bundle member, use a number from 0 to 99. When a QoS group is not associated with a PVC bundle, use numbers greater 100 and greater.
other	All non-configured QoS groups.

Command Default

By default, QoS groups are not associated with PVC bundle members.

Command Modes

PVC bundle-member configuration mode

Command History

Release	Modification
12.4(4)T	This command was introduced to associate a QoS-group with a permanent virtual circuit (PVC) bundle member, using the **qos-group** command in ATM VC bundle-member configuration mode.
12.2(31)SB2	This command was integrated into the Cisco IOS Release 12.2(31)SB2.
12.4(9)XJ	This command modification was integrated into the Cisco IOS Special Release 12.4(9)XJ.
12.4(15)T	This command modification was integrated into the Cisco IOS Release 12.4(6th)T and associates a QoS-group with a permanent virtual circuit (PVC) bundle member in PVC bundle member configuration mode.

Examples

The following example shows the configuration of which QoS groups will use RBE:

```
Router(config-if-atm-member)# qos group 5
```

query certificate

To configure query certificates on a per-trustpoint basis, use the **query certificate** command in ca-trustpoint configuration mode. To disable creation of query certificates per trustpoint, use the **no** form of this command.

query certificate

no query certificate

Syntax Description

This command has no arguments or keywords.

Defaults

Query certificates are stored in NVRAM.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(18)SXE	This command was incorporated into Relese 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

Normally, certain certificates are stored locally in the router's NVRAM, and each certificate uses a moderate amount of memory. To save NVRAM space, you can use this command to prevent certificates from being stored locally; instead, they are retrieved from a specified certification authority (CA) trustpoint when needed. This will save NVRAM space but could result in a slight performance impact.

Before you can configure this command, you must enable the **crypto ca trustpoint** command, which puts you in ca-trustpoint configuration mode.

Using the query certificate Command with a Specific Trustpoint

When the **query certificate** command is used, certificates associated with the specified truspoint will not be written into NVRAM, and the certificate query will be attempted during the next reload of the router.

Applying the Query Mode Globally

When the global command **crypto ca certificate query** command is used, the query certificate will be added to all trustpoints on the router. When the **no crypto ca certificate query** command is used, any previously query certificate configuration will be removed from all trustpoints, and any query in progress will be halted and the feature disabled.

Examples

The following example shows how to configure a trustpoint and initiate query mode for certificate authority:

```
crypto ca trustpoint trustpoint1
 enrollment url http://trustpoint1
 crl query ldap://trustpoint1
 query certificate
 exit
```

Related Commands

Command	Description
crypto ca certificate query	Specifies that certificates should not be stored locally but retrieved from a CA trustpoint.
crypto ca trustpoint	Declares the CA that your router should use.

query url

Note Effective with Cisco IOS Release 12.2(8)T, this command was replaced by the **crl query** command.

If you have to query the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked and you have to provide the Lightweight Directory Access Protocol (LDAP) server information, use the **query url** command in ca-trustpoint configuration mode. To return to the default behavior, assuming that the CRL distribution point (CDP) has a complete (LDAP) URL, use **no** form of this command.

query url ldap://*hostname***:**[*port*]

query url ldap://*hostname***:**[*port*]

Syntax Description

ldap://*hostname*	Query is made to the hostname of the LDAP server that serves the CRL for the certification authority (CA) server (for example, ldap://myldap.cisco.com).
:*port*	(Optional) Port number of the LDAP server (for example, ldap://myldap.cisco.com:3899).

Defaults

No enabled. If **query url ldap://***hostname***:**[*port*] is not enabled, the router assumes that the CDP that is embedded in the certificate is a complete URL (for example, ldap:myldap.cisco.com/CN=myCA,O=Cisco) and uses it to download the CRL.

If the port number is not configured, the default LDAP server port 389 will be used.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(8)T	This command was replaced by the **crl query** command.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When Cisco IOS software tries to verify a peer certificate (for example, during Internet Key Exchange [IKE] or Secure Sockets Layer [SSL] handshake), it queries the CRL to ensure that the certificate has not been revoked. To locate the CRL, it first looks for the CDP extension in the certificate. If the extension exists, it is used to download the CRL. Otherwise, the Simple Certificate Enrollment Protocol (SCEP) GetCRL mechanism is used to query the CRL from the CA server directly (some CA servers do not support this method).

Cisco IOS software supports three types of CDP:

- HTTP URL (Example1: http://10.10.10.10:81/myca.crl)
- LDAP URL (Example 2: ldap://10.10.10.10:3899/CN=myca, O=cisco or Example 3: ldap:///CN=myca, O=cisco)
- LDAP/X.500 DN (Example 4: CN=myca, O=cisco)

To locate the CRL, a complete URL needs to be formed. As a result, Example 3 and Example 4 still require the hostname and the port number. The **ldap://***hostname***:**[*port*} keywords and arguments are used to provide this information.

Note The **crypto ca trustpoint** command replaces the **crypto ca identity** and **crypto ca trusted-root** commands and all related subcommands (all ca-identity and trusted-root configuration mode commands). If you enter a ca-identity or trusted-root subcommand, the configuration mode and command will be written back as ca-trustpoint.

Examples

The following example shows how to configure your router to query the CRL with the LDAP URL that is published by the CA named "bar":

```
crypto ca trustpoint mytp
 enrollment url http://bar.cisco.com
 query url ldap://bar.cisco.com:3899
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
revocation-check	Checks the revocation status of a certificate.

quit

To exit from the key-string mode while defining the Rivest, Shamir, and Adelman (RSA) manual key to be used for encryption or signatures during Internet Key Exchange (IKE) authentication, use the **quit** command in public key configuration mode.

quit

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Public key configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use this command to exit text mode while defining the RSA public key.

Examples

The following example shows that the RSA public key of an IP Security (IPSec) peer has been specified:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```

Related Commands

Command	Description
address	Specifies the IP address of the remote RSA public key of the remote peer that you will manually configure.
key-string (IKE)	Specifies the RSA public key of a remote peer.

radius attribute nas-port-type

To configure subinterfaces such as Ethernet, virtual LANs (VLAN), stacked VLAN (Q-in-Q), virtual circuit (VC), and VC ranges, use the **radius attribute nas-port-type** command in subinterface configuration mode. To disable the subinterface configuration, use the **no** form of this command.

radius attribute nas-port-type *port number*

no radius attribute nas-port-type *port number*

Syntax Description

value	Number assigned for a port type. • The *port number* must be assigned a number 1–40 to set a customized extended NAS-Port Type and configure a specific service port type. Choosing a number outside of this range will force the default NAS port format e string to be used to configure the value for attribute 5 that is sent for that session. • You can set a specific service port type with the **radius-server attribute nas-port format** command. **Note** This setting will override a global NAS-Port-Type session format.

Defaults

NAS-Port-Type is not configured.

Command Modes

Subinterface configuration

Command History

Release	Modification
12.3(7)XI	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

You can override the attribute 61 configured globally at a subinterface level.

To set a different extended attribute 61 value for a subinterface, such as for Ethernet, VLAN, Q-in-Q, VC, or VC ranges, select a value for that port type. An extended attribute 61 setting at a subinterface level will override the global extended attribute 61 value.

Examples

The following example shows how to override the global value set for an extended attribute 61 by setting a separate value of type 30 (PPP over ATM [PPPoA]) on a specific ATM subinterface:

```
Router# configure terminal
Router(config)#
Router(config)# interface atm 5/0/0.1
Router(config-subif)# pvc 1/33
```

```
Router(config-if-atm-vc)#
Router(config-if-atm-vc)# radius attribute nas-port-type 30
```

Related Commands

Command	Description
radius-server attribute 61 extended	Enables extended, non-RFC-compliant NAS-Port-Type attribute (RADIUS attribute 61).
radius-server attribute nas-port format	Sets the NAS-Port format used for RADIUS accounting features and restores the default NAS-Port format, or sets the global attribute 61 session format e string or configures a specific service port type for attribute 61 support.

radius-server accounting system host-config

To enable the router to send a system accounting record for the addition and deletion of a RADIUS server, use the **radius-server accounting system host-config** command in global configuration mode.

To to disable system accounting records, use the **no** form of this command:

radius-server accounting system host-config

no radius-server accounting system host-config

Command Default

The command-level default is not enabled.

Command Modes

Global configuration mode (config)

Command History

Release	Modification
12.4	This command was introduced in Cisco IOS Release 12.4.

Usage Guidelines

The **radius-server accounting system host-config** command is used when configuring RADIUS system accounting on the global RADIUS server.

Examples

The following example shows how RADIUS system accounting is configured with the **radius-server accounting system host-config** command to enable system accounting records on a RADIUS server and private server hosts when they are added or deleted:

```
Router> enable
Router# configure terminal
Router(config)# aaa new-model
Router(config)# radius-server accounting system host-config
Router(config)# aaa group server radius radgroup1
Router(config-sg-radius)# server-private 172.16.1.11 key cisco
Router(config-sg-radius)# accounting system host-config
```

Related Commands

Command	Description
aaa new-model	Enables AAA network security services.
aaa group server radius	Adds the RADIUS server
server-private	Enters the hostname or IP address of the RADIUS server and hidden server key.
accounting system host-config	Enables the generation of system accounting records for private server hosts when they are added or deleted.

radius-server attribute 11 default direction

To specify the default direction of filters from RADIUS, use the **radius-server attribute 11 default direction** command in global configuration mode. To remove this functionality from your configuration, use the **no** form of this command.

radius-server attribute 11 default direction [**inbound** | **outbound**]

no radius-server attribute 11 default direction[**inbound** | **outbound**]

Syntax Description

inbound	(Optional) Filtering is applied to inbound packets only.
outbound	(Optional) Filtering is applied to outbound packets only.

Command Default

This command is disabled by deault.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2(31)SB3	This command was integrated into Cisco IOS Release 12.2(31)SB3.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **radius-server attribute 11 default direction** command to change the default direction of filters from RADIUS (RADIUS attribute 11 (Filter-Id) indicates the name of the filter list for the user). Enabling this command allows you to change the filter direction to inbound—which stops traffic from entering a router and prevents resource consumption—rather than keeping the outbound default direction, where filtering occurs only as the traffic is about to leave the network.

Examples

The following example shows how to configure RADIUS attribute 11 to change the default direction of filters. In this example, the filtering is applied to inbound packets only.

```
radius-server attribute 11 default direction inbound
```

The following is an example of a RADIUS user profile (Merit Daemon format) that includes RADIUS attribute 11 (Filter-Id):

```
client Password = "password1"
        Service-Type = Framed,
        Framed-Protocol = PPP,
        Filter-Id = "myfilter.out"
```

radius-server attribute 188 format non-standard

To send the number of remaining links in the multilink bundle in the accounting-request packet, use the **radius-server attribute 188 format non-standard** command in global configuration mode. To disable the sending of the number of links in the multilink bundle in the accounting-request packet, use the **no** form of this command.

radius-server attribute 188 format non-standard

no radius-server attribute 188 format non-standard

Syntax Description

This command has no arguments or keywords.

Defaults

RADIUS attribute 188 is not sent in accounting “start” and “stop” records.

Command Modes

Global configuration

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to send attribute 188 in accounting “start” and “stop” records.

Examples

The following example shows a configuration that sends RADIUS attribute 188 in accounting-request packets:

```
radius-server attribute 188 format non-standard
```

radius-server attribute 25

To include the class attribute in access-request, use the **radius-server attribute 25** command in global configuration mode. To disable class RADIUS configuration, use the **no** form of this command.

radius-server attribute 25 access-request include

no radius-server attribute 25 access-request include

Syntax Description

access-request	Specifies the default authorization action.
include	Specifies the framed-protocol attribute type.

Command Default

The class atrribute in access-request is not included.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRB.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Attribute 25 refers to class attribute.

Examples

The following example shows how to include the class attribute in access-request:

```
Router# configure terminal
Router(config)# radius-server attribute 25 access-request include
```

Related Commands

Command	Description
radius-server attribute 11 direction default	Specifies the default direction of filters from RADIUS.

radius-server attribute 31

To configure Calling-Station-ID (attribute 31) options, use the **radius-server attribute 31** command in global configuration mode. To disable the Calling-Station-ID (attribute 31) options, use the **no** form of this command.

radius-server attribute 31 {**append-circuit-id** | **mac format** {**default** | **ietf** | **unformatted**} | **remote-id** | **send nas-port-detail** [**mac-only**]}

no radius-server attribute 31 {**append-circuit-id** | **mac format** {**default** | **ietf** | **unformatted**} | **remote-id** | **send nas-port-detail** [**mac-only**]}

Syntax Description

append-circuit-id	Appends the PPPoE tag circuit-id and the nas-port-id to the calling-station-id.
mac format	Specifies the format of the MAC address in the Calling Station ID. Select one of the following three options: • **default** (Example: 0000.4096.3e4a) • **ietf** (Example: 00-00-40-96-3E-4A) • **unformatted** (Example: 000040963e4a)
remote-id	Sends the remote ID as the Calling Station ID in the accounting records and access requests.
send nas-port-detail	Includes all NAS port details in the Calling Station ID.
mac-only	(Optional) Includes the MAC address only, if available, in the Calling Station ID.

Command Default

The Calling-Station-ID (attribute 31) is not sent.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(31)SB2	The **mac format default**, the **mac format ietf**, the **mac format unformatted**, and the **send nas-port-detail** [**mac-only**] keyword options were added.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

- For PPP over Ethernet over ATM (PPPoEoA) sessions:

  When the **send nas-port-detail** keyword and the **mac-only** option are configured, the Calling-Station-ID (attribute 31) information is sent in Access and Accounting requests in the following format:

  ```
  host.domain:vp_descr:vpi:vci
  ```

- For PPP over Ethernet over Ethernet (PPPoEoE) sessions:

  When the **send nas-port-detail** keyword and the **mac-only** option are configured, the Calling-Station-ID (attribute 31) information is sent in Access and Accounting requests in the following format:

  ```
  mac_addr
  ```

- For PPP over ATM sessions:

  When the **send nas-port-detail** keyword and the **mac-only** option are configured, the Calling-Station-ID (attribute 31) information is sent in Access and Accounting requests in the following format:

  ```
  host.domain:vp_descr:vpi:vci
  ```

- For Intelligent Services Gateway RADIUS Proxy sessions:

  When DHCP lease query is used, ISG RADIUS proxy recieves MAC address as well as MSISDN as the Calling-Station-ID (attribute 31) from the downstream device. Therefore, ISG RADIUS proxy must be configured to choose one of them as the Calling Station ID and send it to the ISG accounting records.

The following example shows how to specify the MAC address in the Calling Station ID to be displayed in IETF format:

```
Router(config)# radius-server attribute 31 mac format ietf
```

The following example shows how to allow the remote ID to be sent as the Calling Station ID:

```
Router(config)# radius-server attribute 31 remote-id
```

The following example shows how to allow the NAS port details to be included in the Calling Station ID:

```
Router(config)# radius-server attribute 31 send nas-port-detail
```

The following example shows how to allow only the MAC address, if available, to be included in the Calling-Station-ID:

```
Router(config)# radius-server attribute 31 send nas-port-detail mac-onl
```

Related Commands

Command	Description
radius-server attribute nas-port-id include	Uses the DHCP relay agent information option 60 and option 82 and configures the NAS-Port-ID to authenticate a user.

radius-server attribute 31 mac format

To configure a nondefault MAC address format in the calling line ID (CLID) of a DHCP accounting packet, use the **radius-server attribute 31 mac format** command in global configuration mode. To set the format back to the default MAC address format, use the **no** form of this command.

radius-server attribute 31 mac format {**default** | **ietf** | **unformatted**}

no radius-server attribute 31 mac format {**default** | **ietf** | **unformatted**}

Syntax Description

default	Sets the MAC address format to the default format (for example, aaaa.bbbb.cccc)
ietf	Internet Engineering Task Force (IETF) format (for example, aa-aa-bb-bb-cc-cc).
unformatted	Unformatted raw MAC address (for example, aaaabbbbcccc).

Command Default

If not configured, the format is set to the default format.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2S, 12.3	This command was introduced.

Usage Guidelines

The CLID (attribute 31) is used to carry a variety of information, such as phone numbers, IP addresses, and MAC addresses.

Note The **radius-server attribute 31 send nas-port-detail mac-only** command must also be configured or the CLID will not be sent in the request even if the **radius-server attribute 31 mac format** command is configured.

Examples

The following example shows that the RADIUS calling station ID has been set to “unformatted”:

```
Router# radius-server attribute 31 mac format unformatted
```

Related Commands

Command	Description
radius-server attribute 31 send nas-port-detail mac-only	Configures Calling-Station-ID (attribute 31) options.

radius-server attribute 32 include-in-access-req

To send RADIUS attribute 32 (NAS-Identifier) in an access-request or accounting-request, use the **radius-server attribute 32 include-in-access-req** command in global configuration mode. To disable sending RADIUS attribute 32, use the **no** form of this command.

radius-server attribute 32 include-in-access-req [*format*]

no radius-server attribute 32 include-in-access-req

Syntax Description

format	(Optional) A string sent in attribute 32 containing an IP address (%i), a hostname (%h), or a domain name (%d).

Defaults

RADIUS attribute 32 is not sent in access-request or accounting-request packets.

Command Modes

Global configuration

Command History

Release	Modification
12.1 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Using the **radius-server attribute 32 include-in-access-req** command makes it possible to identify the network access server (NAS) manufacturer to the RADIUS server by sending RADIUS attribute 32 (NAS-Identifier) in an access-request or accounting-request. If you configure the format argument, the string sent in attribute 32 will include an IP address, a hostname, or a domain name; otherwise, the Fully Qualified Domain Name (FQDN) is sent by default.

Examples

The following example shows a configuration that sends RADIUS attribute 32 in the access-request with the format configured to identify a Cisco NAS:

```
radius-server attribute 32 include-in-access-req format cisco %h.%d %i
! The following string will be sent in attribute 32 (NAS-Identifier).
"cisco router.nlab.cisco.com 10.0.1.67"
```

radius-server attribute 4

To configure an IP address for the RADIUS attribute 4 address, use the **radius-server attribute 4** command in global configuration mode. To delete an IP address as the RADIUS attribute 4 address, use the **no** form of this command.

radius-server attribute 4 *ip-address*

no radius-server attribute 4 *ip-address*

Syntax Description

ip-address	IP address to be configured as RADIUS attribute 4 inside RADIUS packets.

Defaults

If this command is not configured, the RADIUS NAS-IP-Address attribute will be the IP address on the interface that connects the network access server (NAS) to the RADIUS server.

Command Modes

Global configuration

Command History

Release	Modification
12.3(3)B	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Normally, when the **ip radius-source interface** command is configured, the IP address on the interface that is specified in the command is used as the IP address in the IP headers of the RADIUS packets and as the RADIUS attribute 4 address inside the RADIUS packets.

However, when the **radius-server attribute 4** command is configured, the IP address in the command is used as the RADIUS attribute 4 address inside the RADIUS packets. There is no impact on the IP address in the IP headers of the RADIUS packets.

If both commands are configured, the IP address that is specified in the **radius-server attribute 4** command is used as the RADIUS attribute 4 address inside the RADIUS packets. The IP address on the interface that is specified in the **ip radius-source interface** command is used as the IP address in the IP headers of the RADIUS packets.

Some authentication, authorization, and accounting (AAA) clients (such as PPP, virtual private dial-up network [VPDN] or Layer 2 Tunneling Protocol [L2TP], Voice over IP [VoIP], or Service Selection Gateway [SSG]) may try to set the RADIUS attribute 4 address using client-specific values. For example, on an L2TP network server (LNS), the IP address of the L2TP access concentrator (LAC) could be specified as the RADIUS attribute 4 address using a VPDN or L2TP command. When the **radius-server attribute 4** command is configured, the IP address specified in the command takes precedence over all IP addresses from AAA clients.

During RADIUS request retransmission and during RADIUS server failover, the specified IP address is always chosen as the value of the RADIUS attribute 4 address.

Examples

The following example shows that the IP address 10.0.0.21 has been configured as the RADIUS NAS-IP-Address attribute:

```
radius-server attribute 4 10.0.0.21
radius-server host 10.0.0.10 auth-port 1645 acct-port 1646 key cisco
```

The following **debug radius** command output shows that 10.0.0.21 has been successfully configured.

```
Router# debug radius

RADIUS/ENCODE(0000001C): acct_session_id: 29
RADIUS(0000001C): sending
RADIUS(0000001C): Send Access-Request to 10.0.0.10:1645 id 21645/17, len 81
RADIUS:  authenticator D0 27 34 C0 F0 C4 1C 1B - 3C 47 08 A2 7E E1 63 2F
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  User-Name           [1]   18  "shashi@pepsi.com"
RADIUS:  CHAP-Password       [3]   19  *
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   10.0.0.21
UDP: sent src=11.1.1.1(21645), dst=10.0.0.10(1645), length=109
UDP: rcvd src=10.0.0.10(1645), dst=10.1.1.1(21645), length=40
RADIUS: Received from id 21645/17 10.0.0.10:1645, Access-Accept, len 32
RADIUS:  authenticator C6 99 EC 1A 47 0A 5F F2 - B8 30 4A 4C FF 4B 1D F0
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS(0000001C): Received from id 21645/17
```

Related Commands

Command	Description
ip radius-source interface	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.

radius-server attribute 44 extend-with-addr

To add the accounting IP address before the existing session ID, use the **radius-server attribute 44 extend-with-addr** command in global configuration mode. To remove this command from your configuration, use the **no** form of this command.

radius-server attribute 44 extend-with-addr

no radius-server attribute 44 extend-with-addr

Syntax Description

This command has no arguments or keywords.

Defaults

This command is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The **radius-server attribute 44 extend-with-addr** command adds Acct-Session-Id (attribute 44) before the existing session ID (NAS-IP-Address).

When multiple network access servers (NAS) are being processed by one offload server, enable this command on all NASs and the offload server to ensure a common and unique session ID.

Note This command should be enabled only when offload servers are used.

Examples

The following example shows how to configure unique session IDs among NASs:

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server attribute 44 extend-with-addr
```

Related Commands

Command	Description
radius-server attribute 44 include-in-access-req	Sends RADIUS attribute 44 (Acct-Session-Id) in access-request packets before user authentication.
radius-server attribute 44 sync-with-client	Configures the offload server to synchronize accounting session information with the NAS clients.

radius-server attribute 44 include-in-access-req

To send RADIUS attribute 44 (Accounting Session ID) in access request packets before user authentication (including requests for preauthentication), use the **radius-server attribute 44 include-in-access-req** command in global configuration mode. To remove this command from the configuration, use the **no** form of this command.

radius-server attribute 44 include-in-access-req [**vrf** *vrf-name*]

no radius-server attribute 44 include-in-access-req [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Per VRF configuration.

Defaults

RADIUS attribute 44 is not sent in access-request packets.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(1)DX	The **vrf** keyword and *vrf-name* argument were introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

There is no guarantee that the Accounting Session IDs will increment uniformly and consistently. In other words, between two calls, the Accounting Session ID can increase by more than one.

The **vrf** *vrf-name* keyword and argument specify Accounting Session IDs per Virtual Private Network (VPN) routing and forwarding (VRF), which allows multiple disjoined routing or forwarding tables, where the routes of a user have no correlation with the routes of another user.

Examples

The following example shows a configuration that sends RADIUS attribute 44 in access-request packets:

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server attribute 44 include-in-access-req
```

radius-server attribute 44 sync-with-client

To configure the offload server to synchronize accounting session information with the network access server (NAS) clients, use the **radius-server attribute 44 sync-with-client** command in global configuration mode. To disable this functionality, use the **no** form of this command.

radius-server attribute 44 sync-with-client

no radius-server attribute 44 sync-with-client

Syntax Description

This command has no arguments or keywords.

Command Default

This command is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Use the **radius-server attribute 44 sync-with-client** command to allow the offload server to synchronize accounting session information with the NAS clients. The NAS-IP-Address, the Acct-Session-Id, and the Class attribute are transmitted from the client to the offload server via Layer 2 Forwarding (L2F) options.

Examples

The following example shows how to configure the offload server to synchronize accounting session information with the NAS clients:

```
radius-server attribute 44 sync-with-client
```

Related Commands

Command	Description
radius-server attribute 44 extend-with-addr	Adds the accounting IP address before the existing session ID.
radius-server attribute 44 include-in-access-req	Sends RADIUS attribute 44 (Acct-Session-Id) in access-request packets before user authentication.

radius-server attribute 55 include-in-acct-req

To send the RADIUS attribute 55 (Event-Timestamp) in accounting packets, use the **radius-server attribute 55 include-in-acct-req** command in global configuration mode. To remove this command from your configuration, use the **no** form of this command.

radius-server attribute 55 include-in-acct-req

no radius-server attribute 55 include-in-acct-req

Syntax Description

This command has no arguments or keywords.

Defaults

RADIUS attribute 55 is not sent in accounting packets.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **radius-server attribute 55 include-in-acct-req** command to send RADIUS attribute 55 (Event-Timestamp) in accounting packets. The Event-Timestamp attribute records the time that the event occurred on the NAS; the timestamp sent in attribute 55 is in seconds since January 1, 1970 00:00 UTC.

Note Before the Event-Timestamp attribute can be sent in accounting packets, you *must* configure the clock on the router. (For information on setting the clock on your router, refer to section "Performing Basic System Management" in the chapter "System Management" of the *Cisco IOS Configuration Fundamentals and Network Management Configuration Guide*.)

To avoid configuring the clock on the router every time the router is reloaded, you can enable the **clock calendar-valid** command. (For information on this command, refer to the *Cisco IOS Configuration Fundamentals and Network Management Command Reference.*)

Examples

The following example shows how to enable your router to send the Event-Timestamp attribute in accounting packets. (To see whether the Event-Timestamp was successfully enabled, use the **debug radius** command.)

```
radius-server attribute 55 include-in-acct-req
```

Related Commands

Command	Description
clock calendar-valid	Configures a system as an authoritative time source for a network based on its hardware clock (calendar).
clock set	Manually sets the system software clock.

radius-server attribute 6

To provide for the presence of the Service-Type attribute (attribute 6) in RADIUS Access-Accept messages, use the **radius-server attribute 6** command in global configuration mode. To make the presence of the Service-Type attribute optional in Access-Accept messages, use the **no** form of this command.

radius-server attribute 6 {**mandatory** | **on-for-login-auth** | **support-multiple** | **voice** *value*}

no radius-server attribute 6 {**mandatory** | **on-for-login-auth** | **support-multiple** | **voice** *value*}

Syntax Description

mandatory	Makes the presence of the Service-Type attribute mandatory in RADIUS Access-Accept messages.
on-for-login-auth	Sends the Service-Type attribute in the authentication packets. **Note** The Service-Type attribute is sent by default in RADIUS Accept-Request messages. Therefore, RADIUS tunnel profiles should include "Service-Type=Outbound" as a check item, not just as a reply item. Failure to include Service-Type=Outbound as a check item can result in a security hole.
support-multiple	Supports multiple Service-Type values for each RADIUS profile.
voice *value*	Selects the Service-Type value for voice calls. The only value that can be entered is 1. The default is 12.

Command Default

If this command is not configured, the absence of the Service-Type attribute is ignored, and the authentication or authorization does not fail. The default for the **voice** keyword is 12.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.2(13)T	The **mandatory** keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If this command is configured and the Service-Type attribute is absent in the Access-Accept message packets, the authentication or authorization fails.

The **support-multiple** keyword allows for multiple instances of the Service-Type attribute to be present in an Access-Accept packet. The default behavior is to disallow multiple instances, which results in an Access-Accept packet containing multiple instances being treated as though an Access-Reject was received.

Examples

The following example shows that the presence of the Service-Type attribute is mandatory in RADIUS Access-Accept messages:

```
Router(config)# radius-server attribute 6 mandatory
```

The following example shows that attribute 6 is to be sent in authentication packets:

```
Router(config)# radius-server attribute 6 on-for-login-auth
```

The following example shows that multiple Service-Type values are to be supported for each RADIUS profile:

```
Router(config)# radius-server attribute 6 support-multiple
```

The following example shows that Service-Type values are to be sent in voice calls:

```
Router(config)# radius-server attribute 6 voice 1
```

radius-server attribute 61 extended

To enable extended, non-RFC-compliant NAS-Port-Type attribute (RADIUS attribute 61), use the **radius-server attribute 61 extended** command in global configuration mode. To disable extended, non-RFC-compliant NAS-Port-Type attribute (RADIUS attribute 61), use the **no** form of this command.

radius-server attribute 61 extended

no radius-server attribute 61 extended

Syntax Description

This command has no arguments or keywords.

Defaults

Extended attribute 61 is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)XI1	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

RADIUS Attribute 61 (Network-attached storage (NAS) port-type, a number) is sent in an access-request to indicate the type of physical port of the NAS, which is authenticating the user with number.

Table 57 NAS Access Technology Values

RADIUS Value	Service Port Type
27	Wireless - IEEE 802.16
30	PPP over ATM (PPPoA)
31	PPP over Ethernet over ATM (PPPoEoA)
32	PPP over Ethernet over Ethernet (PPPoEoE)
33	PPP over Ethernet over VLAN (PPPoEoVLAN)
34	Point-to-Point Protocol over Ethernet IEEE 802.1Q Tunneling (PPPoEoQinQ)

The Value "Virtual" refers to a connection to the NAS through a transport protocol, instead of through a physical port. For example, if a user telnetted into a NAS, the value "Virtual" would be reflected as the NAS value.

There is no specific NAS value for IP sessions. The NAS value depends on the underlying transport technology values described in Table 57 or "Virtual" is used for IP sessions. For example, if PPP is the underlying access technology (transport protocol), the value reported is 33.

If extended attribute 61 is not enabled the following occurs:

- All PPPoA, PPPoE, PPPoEoE, PPPoEoA sessions are identified as “Virtual”.
- All PPPoEoVLAN and PPPoEoQinQ sessions are identified as VLAN.
- RFC-compliant values, such as Virtual (value 5) and Ethernet (value 15) are sent to the authentication, authorization, and accounting (AAA) records.

Examples

The following example shows how to configure global support for extended attribute 61 ports and how to specify different format e strings globally for two different types of ports:

- Type 30 (which is PPPoA)
- Type 33 (which is PPPoEoVLAN)

```
Router# configure terminal
Router(config)#
Router(config)# radius-server attribute 61 extended
Router(config)# radius-server attribute nas-port format e SSSSAPPPUUUUUUUUUUUUUUUUUUUUUUUUUU
Router(config)# radius-server attribute nas-port format e SSSSAPPPIIIIIIIICCCCCCCCCCCCCCCC
type 30
Router(config)#
Router(config)# radius-server attribute nas-port format e SSSSAPPPVVVVVVVVVVVVVVVVVVVVVVVV
type 33
Router(config)#
```

Related Commands

Command	Description
radius attribute nas-port-type	Configures subinterfaces such as Ethernet, VLANS, stacked VLAN (Q-in-Q), VC and VC ranges.
radius-server attribute nas-port format	Sets the NAS-Port format used for RADIUS accounting features and restores the default NAS-Port format, or sets the global attribute 61 session format e string or configures a specific service port type for attribute 61 support.

radius-server attribute 69 clear

To receive nonencrypted tunnel passwords in attribute 69 (Tunnel-Password), use the **radius-server attribute 69 clear** command in global configuration mode. To disable this feature and receive encrypted tunnel passwords, use the **no** form of this command.

radius-server attribute 69 clear

no radius-server attribute 69 clear

Syntax Description

This command has no arguments or keywords.

Defaults

RADIUS attribute 69 is not sent and encrypted tunnel passwords are sent.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **radius-server attribute 69 clear** command to receive nonencrypted tunnel passwords, which are sent in RADIUS attribute 69 (Tunnel-Password). This command allows tunnel passwords to be sent in a "string" encapsulated format, rather than the standard tag/salt/string format, which enables the encrypted tunnel password.

Some RADIUS servers do not encrypt Tunnel-Password; however the current NAS (network access server) implementation will decrypt a non-encrypted password that causes authorization failures. Because nonencrypted tunnel passwords can be sent in attribute 69, the NAS will no longer decrypt tunnel passwords.

Note Once this command is enabled, all tunnel passwords received will be nonencrypted until the command is manually disabled.

Examples

The following example shows how to enable attribute 69 to receive nonencrypted tunnel passwords. (To see whether the Tunnel-Password process is successful, use the **debug radius** command.)

```
radius-server attribute 69 clear
```

radius-server attribute 77

To send connection speed information to the RADIUS server in the access request, use the **radius-server attribute 77** command in global configuration mode. To prevent connection speed information from being included in the access request, use the **no** form of this command.

radius-server attribute 77 {include-in-access-req | include-in-acct-req}

no radius-server attribute 77 {include-in-access-req | include-in-acct-req}

Syntax Description

include-in-access-req	Specifies that attribute 77 will be included in access requests.
include-in-acct-req	Specifies that attribute 77 will be included in accounting requests.

Defaults

RADIUS attribute 77 is sent to the RADIUS server in the access request.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)BX	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

RADIUS attribute 77 is sent to the RADIUS server in the access request by default.

RADIUS attribute 77 allows RADIUS authentication based on connection speed. Sessions can be accepted or denied based on the allowed connection speed configured for a particular user on the RADIUS server.

RADIUS attribute 77 includes the following information:

- The accounting start/stop request
- The VC class name defined with the **class-int** command
- The VC class name defined with the **class-vc** command
- The VC class name defined with the **class-range** command

The VC class name may include letters, numbers, and the characters ":" (colon), ";" (semicolon), "-" (hyphen) and "," (comma).

Examples

The following example disables the inclusion of RADIUS attribute 77 in the access request:

```
no radius-server attribute 77 include-in-access-req
```

Related Commands

Command	Description
class-int	Assigns a VC class to an ATM main interface or subinterface.
class-range	Assigns a VC class to an ATM PVC range.
class-vc	Assigns a VC class to an ATM PVC, SVC, or VC bundle member.

radius-server attribute 8 include-in-access-req

To send the IP address of a user to the RADIUS server in the access request, use the **radius-server attribute 8 include-in-access-req** command in global configuration mode. To disable sending of the user IP address to the RADIUS server during authentication, use the **no** form of this command.

radius-server attribute 8 include-in-access-req

no radius-server attribute 8 include-in-access-req

Syntax Description

This command has no arguments or keywords.

Defaults

This feature is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Using the **radius-server attribute 8 include-in-access-req** command makes it possible for a network access server (NAS) to provide the RADIUS server with a hint of the user IP address in advance of user authentication. An application can be run on the RADIUS server to use this hint and build a table (map) of user names and addresses. Using the mapping information, service applications can begin preparing user login information to have available upon successful user authentication.

When a network device dials in to a NAS that is configured for RADIUS authentication, the NAS begins the process of contacting the RADIUS server in preparation for user authentication. Typically, the IP address of the dial-in host is not communicated to the RADIUS server until after successful user authentication. Communicating the device IP address to the server in the RADIUS access request allows other applications to begin to take advantage of that information.

As the NAS is setting up communication with the RADIUS server, the NAS assigns an IP address to the dial-in host from a pool of IP addresses configured at the specific interface. The NAS sends the IP address of the dial-in host to the RADIUS server as attribute 8. At that time, the NAS sends other user information, such as the username, to the RADIUS server.

After the RADIUS server receives the user information from the NAS, it has two options:

- If the user profile on the RADIUS server already includes attribute 8, the RADIUS server can override the IP address sent by the NAS with the IP address defined as attribute 8 in the user profile. The address defined in the user profile is returned to the NAS.

- If the user profile does not include attribute 8, the RADIUS server can accept attribute 8 from the NAS, and the same address is returned to the NAS.

The address returned by the RADIUS server is saved in memory on the NAS for the life of the session. If the NAS is configured for RADIUS accounting, the accounting start packet sent to the RADIUS server includes the same IP address as in attribute 8. All subsequent accounting packets, updates (if configured), and "stop" packets will also include the same IP address as in attribute 8.

Note Configuring the NAS to send the host IP address in the RADIUS access request assumes that the login host is configured to request an IP address from the NAS server. It also assumes that the login host is configured to accept an IP address from the NAS. In addition, the NAS must be configured with a pool of network addresses at the interface supporting the login hosts.

Examples

The following example shows a NAS configuration that sends the IP address of the dial-in host to the RADIUS server in the RADIUS access request. The NAS is configured for RADIUS authentication, authorization, and accounting (AAA). A pool of IP addresses (async1-pool) has been configured and applied at interface Async1.

```
aaa new-model
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
!
ip address-pool local
!
interface Async1
 peer default ip address pool async1-pool
!
ip local pool async1-pool 209.165.200.225 209.165.200.229
!
radius-server host 172.31.71.146 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute 8 include-in-access-req
radius-server key radhost
```

radius-server attribute 30 original-called-number

To allow network providers to accurately match the billing function with the actual number dialed (Original Called Number (OCN)), and not the translated number to which the switch reports, use the **radius-server attribute 30 original-called-number** command in global configuration mode.

radius-server attribute 30 original-called-number

no radius-server attribute 30 original-called-number

Command Default

The command-level default is not enabled. The translated number is sent to the NAS.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3	This command was introduced.

Usage Guidelines

The ITU-T Q.931 attribute is the connection control protocol of the ISDN. Some switches can send a translated dialed number identification service (DNIS) number to the network access server (NAS) instead of the OCN. These switches eventually inform the NAS about the OCN in its Q931 attribute. However, some network providers require the OCN in its Q.931 attribute.

The **radius-server attribute 30 original-called-number** command allows the OCN with its Q.931 attribute to be sent to the RADIUS Called-Station-ID, which is a check mechanism administrators use to deny or accept access from users based on the NAS (when available). This OCN is used instead of the redirected translated number reported as the DNIS by ISDN.

Examples

The following example enables the **radius-server attribute 30 original-called-number** in global configuration mode:

```
aaa new-model
radius-server attribute 30 original-called-number
```

radius-server attribute data-rate send 0

Note Effective with Cisco IOS Release 12.4, the **radius-server attribute data-rate send 0** command is not available in Cisco IOS software.

To enable the data transmit and receive rate of RADIUS server attributes 197 and 255 in accounting records, use the **radius-server attribute data-rate send 0** command in global configuration mode.

radius-server attribute data-rate send 0

no radius-server attribute data-rate send 0

Syntax Description

This command has no arguments or keywords.

Command Default

The default value for RADIUS server attributes 197 and 255 is zero.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3	This command was introduced.
12.4	This command was removed.

Usage Guidelines

RADIUS attribute 197 is the Ascend-Data-Rate in an accounting-request packet. This attribute specifies the receive baud rate of the connection in bits per second over the course of the connection's lifetime.

RADIUS attribute 255 is the Ascend-Xmit-Rate in an accounting-request packet. This attribute specifies the transmit baud rate of the connection in bits per second over the course of the connection’s lifetime.

The connection is authenticated for both RADIUS attributes 197 and 255 if the following conditions are met:

- The session has ended or has failed to authenticate because the accounting-request packet has the RADIUS attribute: Acct-Status-Type=Stop.
- The Auth parameter is set to a value other than RADIUS or LOGOUT.

Note RADIUS attribute 197 does not appear in the user profile.

Examples

The following example enables the **radius-server attribute data-rate send 0** command in global configuration mode:

```
aaa new-model
radius-server attribute data-rate send 0
```

radius-server attribute list

To define an accept or reject list name, use the **radius-server attribute list** command in global configuration mode. To remove an accept or reject list name from your configuration, use the **no** form of this command.

radius-server attribute list *list-name*

no radius-server attribute list *list-name*

Syntax Description

list-name	Name for an accept or reject list.

Command Default

List names are not defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(1)DX	This command was introduced.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(13)T	Platform support was added for the Cisco 7401 ASR router.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.3S.	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

A user may configure an accept or reject list with a selection of attributes on the network access server (NAS) for authorization or accounting so unwanted attributes are not accepted and processed. The **radius-server attribute list** command allows users to specify a name for an accept or reject list. This command is used in conjunction with the **attribute** (server-group configuration) command, which adds attributes to an accept or reject list.

Note The list name must be the same as the list name defined in the **accounting** or **authorization** configuration command.

Examples

The following example shows how to configure the reject list "bad-list" for RADIUS authorization and accept list "usage-only" for RADIUS accounting:

```
Router(config)# aaa new-model
Router(config)# aaa authentication ppp default group radius-sg
Router(config)# aaa authorization network default group radius-sg
Router(config)# aaa group server radius radius-sg
Router(config-sg-radius)# server 10.1.1.1
Router(config-sg-radius)# authorization reject bad-list
Router(config-sg-radius)# accounting accept usage-only
Router(config-sg-radius)# exit
Router(config)# radius-server host 10.1.1.1 key mykey1
Router(config)# radius-server attribute list usage-only
Router(config-radius-attrl)# attribute 1,40,42-43,46
Router(config-radius-attrl)# exit
Router(config)# radius-server attribute list bad-list
Router(config-radius-attrl)# attribute 22,27-28,56-59
```

Note Although you cannot configure more than one access or reject list per server group for authorization or accounting, you can configure one list for authorization and one list for accounting per server group.

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
accounting (server-group configuration)	Specifies an accept or reject list for attributes that are to be sent to the RADIUS server in an accounting request.
attribute (server-group configuration)	Adds attributes to an accept or reject list.
authorization (server-group configuration)	Specifies an accept or reject list for attributes that are returned in an Access-Accept packet from the RADIUS server.
radius-server host	Specifies a RADIUS server host.

radius-server attribute nas-port extended

The **radius-server attribute nas-port extended** command is replaced by the **radius-server attribute nas-port format** command. See the description of the **radius-server attribute nas-port format** command for more information.

radius-server attribute nas-port format

To set the NAS-Port format used for RADIUS accounting features and restore the default NAS-port format, or to set the global attribute 61 session format e string or configure a specific service port type for attribute 61 support, use the **radius-server attribute nas-port format** command in global configuration mode. To stop sending attribute 61 to the RADIUS server, use the **no** form of this command.

NAS-Port for RADIUS Accounting Features and Restoring Default NAS-Port Format

radius-server attribute nas-port format *format*

no radius-server attribute nas-port format *format*

Extended NAS-Port Support

radius-server attribute nas-port format *format* [*string*] [**type** *nas-port-type*]

no radius-server attribute nas-port format *format* [*string*] [**type** *nas-port-type*]

Syntax Description

format	NAS-Port format. Possible values for the format argument are as follows: • a—Standard NAS-Port format • b—Extended NAS-Port format • c—Carrier-based format • d—PPPoX (PPP over Ethernet or PPP over ATM) extended NAS-Port format • e—Configurable NAS-Port format
string	(Optional) Represents all of a specific port type for format e. It is possible to specify multiple values with this argument.
type *nas-port-type*	(Optional) Allows you to globally specify different format strings to represent specific physical port types. You may set one of the extended NAS-Port-Type attribute values: • **type 30**—PPP over ATM (PPPoA) • **type 31**—PPP over Ethernet (PPPoE) over ATM (PPPoEoA) • **type 32**—PPPoE over Ethernet (PPPoEoE) • **type 33**—PPPoE over VLAN (PPPoEoVLAN) • **type 34**—PPPoE over Q-in-Q (PPPoEoQinQ)

Defaults

Standard NAS-Port format for NAS-Port for RADIUS accounting features and restoring default NAS-Port format or extended NAS-Port support.

Command Modes

Global configuration

Command History

Release	Modification
11.3(7)T	This command was introduced.
11.3(9)DB	The PPP extended NAS-Port format was added.
12.1(5)T	The PPP extended NAS-Port format was expanded to support PPPoE over ATM and PPPoE over IEEE 802.1Q VLANs.
12.2(4)T	Format e was introduced.
12.2(11)T	Format e was extended to support PPPoX information.
12.3(3)	Format e was extended to support Session ID U.
12.3(7)XI1	Format e was extended to allow the format string to be NAS-Port-Type attribute specific. The following keyword and arguments were added: *string,* **type** *nas-port-type.*
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The **radius-server attribute nas-port format** command configures RADIUS to change the size and format of the NAS-Port attribute field (RADIUS IETF attribute 5).

The following NAS-Port formats are supported:

- Standard NAS-Port format—This 16-bit NAS-Port format indicates the type, port, and channel of the controlling interface. This is the default format used by Cisco IOS software.
- Extended NAS-Port format—The standard NAS-Port attribute field is expanded to 32 bits. The upper 16 bits of the NAS-Port attribute display the type and number of the controlling interface; the lower 16 bits indicate the interface that is undergoing authentication.
- Shelf-slot NAS-Port format—This 16-bit NAS-Port format supports expanded hardware models requiring shelf and slot entries.
- PPP extended NAS-Port format—This NAS-Port format uses 32 bits to indicate the interface, virtual path identifier (VPI), and virtual channel indicator (VCI) for PPPoA and PPPoEoA, and the interface and VLAN ID for PPPoE over Institute of Electrical and Electronic Engineers (IEEE) standard 802.1Q VLANs.

Format e

Before Cisco IOS Release 12.2(4)T formats a through c did not work with Cisco platforms such as the AS5400. For this reason, a configurable format e was developed. Format e requires you to explicitly define the usage of the 32 bits of attribute 25 (NAS-Port). The usage is defined with a given parser character for each NAS-Port field of interest for a given bit field. By configuring a single character in a

row, such as x, only one bit is assigned to store that given value. Additional characters of the same type, such as x, will provide a larger available range of values to be stored. Table 58 shows how the ranges may be expanded:

Table 58 Format e Ranges

Character	Range
x	0–1
xx	0–3
xxx	0–7
xxxx	0–F
xxxxx	0–1F

It is imperative that you know what the valid range is for a given parameter on a platform that you want to support. The Cisco IOS RADIUS client will bitmask the determined value to the maximum permissible value on the basis of configuration. Therefore, if one has a parameter that turns out to have a value of 8, but only 3 bits (xxx) are configured, 8 and 0x7 will give a result of 0. Therefore, you must always configure a sufficient number of bits to capture the value required correctly. Care must be taken to ensure that format e is configured to properly work for all NAS port types within your network environment.

Table 59 shows the supported parameters and their characters:

Table 59 Supported Parameters and Characters

Supported Parameters	Characters
Zero	0 (always sets a 0 to that bit)
One	1 (always sets a 0 to that bit)
DS0 shelf	f
DS0 slot	s
DS0 adaptor	a
DS0 port	p (physical port)
DS0 subinterface	i
DS0 channel	c
Async shelf	F
Async slot	S
Async port	P
Async line	L (modern line number, that is, physical terminal [TTY] number)
PPPoX slot	S
PPPoX adaptor	A
PPPoX port	P
PPPoX VLAN ID	V
PPPoX VPI	I

Table 59 Supported Parameters and Characters

Supported Parameters	Characters
PPPoX VCI	C
Session ID	U

All 32 bits that represent the NAS-Port must be set to one of the above characters because this format makes no assumptions for empty fields.

Access Router

The DS0 port on a T1-based card and on a T3-based card will give different results. On T1-based cards, the physical port is equal to the virtual port (because these are the same). So, p and d will give the same information for a T1 card. However, on a T3 system, the port will give you the physical port number (because there can be more than one T3 card for a given platform). As such, d will give you the virtual T1 line (as per configuration on a T3 controller). On a T3 system, p and d will be different, and one should capture both to properly identify the physical device. As a working example for the Cisco AS5400, the following configuration is recommended:

```
Router (config)# radius-server attribute nas-port format e SSSSPPPPPPPPPsssspppppccccc
```

This will give one an asynchronous slot (0–16), asynchronous port (0–512), DS0 slot (0–16), DS0 physical port (0–32), DS0 virtual port (0–32), and channel (0–32). The parser has been implemented to explicitly require 32-bit support, or it will fail.

Finally, format e is supported for channel-associated signaling (CAS), PRI, and BRI–based interfaces.

Note This command replaces the **radius-server attribute nas-port extended** command.

Extended NAS-Port-Type Attribute Support

This command allows you to configure a specific service port type for extended attribute 61 support which overrides the default global setting.

Examples

In the following example, a RADIUS server is identified, and the NAS-Port field is set to the PPP extended format:

```
radius-server host 192.0.2.96 auth-port 1645 acct-port 1646
radius-server attribute nas-port format d
```

The following example shows how to configure global support for extended NAS-Port-Type ports and how to specify two separate format e strings globally for two different types of ports:

- type 30 (which is PPPoA)
- type 33 which is (PPPoEoVLAN)

```
Router# configure terminal
Router(config)#
Router(config)# radius-server attribute 61 extended
Router(config)# radius-server attribute nas-port format e SSSSAPPPUUUUUUUUUUUUUUUUUUUUUUUUUU
Router(config)# radius-server attribute nas-port format e SSSSAPPPIIIIIIIICCCCCCCCCCCCCCCC
type 30
Router(config)#
Router(config)# radius-server attribute nas-port format e SSSSAPPPVVVVVVVVVVVVVVVVVVVVVVVV
type 33
```

Related Commands

Command	Description
radius attribute nas-port-type	Configures subinterfaces such as Ethernet, vLANs, stacked VLAN (Q-in-Q), virtual circuit (VC), and VC ranges.
radius-server attribute 61 extended	Enables extended, non-RFC-compliant NAS-Port-Type attribute (RADIUS attribute 61).
vpdn aaa attribute	Enables the LNS to send PPP extended NAS-Port format values to the RADIUS server for accounting.

radius-server authorization

To set the default framed protocol in the RADIUS packet to Point-toPoint Protocol (PPP), use the **radius-server authorization** command in global configuration mode. To disable the authorization, use the **no** form of this command.

radius-server authorization default framed-protocol ppp

no radius-server authorization default framed-protocol ppp

Syntax Description

default	Specifies the default authorization action.
framed-protocol	Specifies the framed-protocol attribute type.
ppp	Specifies the service port type for the default authorization action.

Command Default

The defualt framed protocol in the RADIUS packet to PPP is not set.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRB	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRB.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Examples

The following example shows how to set the default framed protocol in RADIUS packet to PPP:

```
Router# configure terminal
Router(config)# radius-server authorization default framed-protocol ppp
```

Related Commands

Command	Description
radius-server attribute 6	Provides for the presence of the Service-Type attribute (attribute 6) in RADIUS Access-Accept messages.

radius-server authorization missing Service-Type

The **radius-server authorization missing Service-Type** command is replaced by the **radius-server attribute 6** command. See the **radius-server attribute 6** command for more information.

radius-server backoff exponential

To configure the router for exponential backoff retransmit of accounting requests, use the **radius-server backoff exponential** command in global configuration mode. To disable this functionality, use the **no** form of this command.

radius-server backoff exponential [**max-delay** *minutes*] [**backoff-retry** *retransmits*]

no radius-server backoff exponential [**max-delay** *minutes*] [**backoff-retry** *retransmits*]

Syntax Description

max-delay *minutes*	(Optional) Number of retransmissions done in exponential max-delay mode. Valid range for the *minutes* argument is 1 through 120; if this option is not specified, the default value (60 minutes) will be used.
backoff-retry *retransmits*	(Optional) Number of retransmissions done in exponential backoff mode in addition to normal and max-delay retransmissions. Valid range for the *retransmits* argument is 1 through 50; if this option is not specified, the default value (5 retransmits) will be used.

Command Default

This command is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)B	This command was introduced on the Cisco 6400-NRP-1, Cisco 7200 series, and Cisco 7400 series.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The **radius-server backoff exponential** command is used to keep accounting records on a router for up to 24 hours. After enabling this command, the router will try to send the normal retransmissions for the number of times the *retransmits* argument is configured. Thereafter, the router will continue to retransmit accounting requests with an interval that doubles on each retransmit failure until a configured maximum interval is reached.

While the router is in "retransmit mode," it will store all accounting records that are generated during that period in its memory; the accounting records will be sent to the RADIUS server after the router comes back up before the retransmit mode is complete.

Examples

The following example shows how to configure your router for exponential backoff retransmit of accounting requests:

```
aaa new-model
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authorization exec default group radius
```

```
aaa authorization network default group radius
aaa accounting send stop-record authentication failure
aaa accounting update periodic 1
aaa accounting network default start-stop group radius
!
interface BRI1/0
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
 no ip mroute-cache
 dialer idle-timeout 0
 dialer-group 1
 isdn switch-type basic-5ess
!
radius-server host 172.107.164.206 auth-port 1645 acct-port 1646 backoff exponential
max-delay 60 backoff-retry 32
radius-server backoff exponential max-delay 60 backoff-retry 32
radius-server retransmit 3
radius-server key rad123
end
```

Related Commands

Command	Description
backoff exponential	Configures the router for exponential backoff retransmit of accounting requests per RADIUS server group.
radius-server host	Specifies a RADIUS server host.

radius-server challenge-noecho

To prevent user responses to Access-Challenge packets from being displayed on the screen, use the **radius-server challenge-noecho** command in global configuration mode. To return to the default condition, use the **no** form of this command.

radius-server challenge-noecho

no radius-server challenge-noecho

Syntax Description

This command has no arguments or keywords.

Defaults

All user responses to Access-Challenge packets are echoed to the screen.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies to all users. When the **radius-server challenge-noecho** command is configured, user responses to Access-Challenge packets are not displayed unless the Prompt attribute in the user profile is set to *echo* on the RADIUS server. The Prompt attribute in a user profile overrides the **radius-server challenge-noecho** command for the individual user. For more information, see the chapter "Configuring RADIUS" in the *Cisco IOS Security Configuration Guide*.

Examples

The following example stops all user responses from displaying on the screen:

```
radius-server challenge-noecho
```

radius-server configure-nas

To have the Cisco router or access server query the vendor-proprietary RADIUS server for the static routes and IP pool definitions used throughout its domain when the device starts up, use the **radius-server configure-nas** command in global configuration mode. To discontinue the query of the RADIUS server, use the **no** form of this command.

radius-server configure-nas

no radius-server configure-nas

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **radius-server configure-nas** command to have the Cisco router query the vendor-proprietary RADIUS server for static routes and IP pool definitions when the router first starts up. Some vendor-proprietary implementations of RADIUS let the user define static routes and IP pool definitions on the RADIUS server instead of on each individual network access server in the network. As each network access server starts up, it queries the RADIUS server for static route and IP pool information. This command enables the Cisco router to obtain static routes and IP pool definition information from the RADIUS server.

Note Because the **radius-server configure-nas** command is performed when the Cisco router starts up, it will not take effect until you issue a **copy system:running-config nvram:startup-config** command.

Examples

The following example shows how to tell the Cisco router or access server to query the vendor-proprietary RADIUS server for already-defined static routes and IP pool definitions when the device first starts up:

```
radius-server configure-nas
```

Related Commands

Command	Description
radius-server host non-standard	Identifies that the security server is using a vendor-proprietary implementation of RADIUS.

radius-server dead-criteria

To force one or both of the criteria—used to mark a RADIUS server as dead—to be the indicated constant, use the **radius-server dead-criteria** command in global configuration mode. To disable the criteria that were set, use the **no** form of this command.

radius-server dead-criteria [**time** *seconds*] [**tries** *number-of-tries*]

no radius-server dead-criteria [**time** *seconds* | **tries** *number-of-tries*]

Syntax Description

time *seconds*	(Optional) Minimum amount of time, in seconds, that must elapse from the time that the router last received a valid packet from the RADIUS server to the time the server is marked as dead. If a packet has not been received since the router booted, and there is a timeout, the time criterion will be treated as though it has been met. You can configure the time to be from 1 through 120 seconds. • If the *seconds* argument is not configured, the number of seconds will range from 10 to 60 seconds, depending on the transaction rate of the server. **Note** Both the time criterion and the tries criterion must be met for the server to be marked as dead.
tries *number-of-tries*	(Optional) Number of consecutive timeouts that must occur on the router before the RADIUS server is marked as dead. If the server performs both authentication and accounting, both types of packets will be included in the number. Improperly constructed packets will be counted as though they were timeouts. All transmissions, including the initial transmit and all retransmits, will be counted. You can configure the number of timeouts to be from 1 through 100. • If the *number-of-tries* argument is not configured, the number of consecutive timeouts will range from 10 to 100, depending on the transaction rate of the server and the number of configured retransmissions. **Note** Both the time criterion and the tries criterion must be met for the server to be marked as dead.

Command Default

The number of seconds and number of consecutive timeouts that occur before the RADIUS server is marked as dead will vary, depending on the transaction rate of the server and the number of configured retransmissions.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced.

Release	Modification
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Note Both the time criterion and the tries criterion must be met for the server to be marked as dead.

The **no** form of this command has the following cases:

- If neither the *seconds* nor the *number-of-tries* argument is specified with the **no radius-server dead-criteria** command, both time and tries will be reset to their defaults.
- If the *seconds* argument is specified using the originally set value, the time will be reset to the default value range (10 to 60).
- If the *number-of-tries* argument is specified using the originally set value, the number of tries will be reset to the default value range (10 to 100).

Examples

The following example shows how to configure the router so that it will be considered dead after 5 seconds and 4 tries:

```
Router (config)# radius-server dead-criteria time 5 tries 4
```

The following example shows how to disable the time and number-of-tries criteria that were set for the **radius-server dead-criteria** command.

```
Router (config)# no radius-server dead-criteria
```

The following example shows how to disable the time criterion that was set for the **radius-server dead-criteria** command.

```
Router (config)# no radius-server dead-criteria time 5
```

The following example shows how to disable the number-of-tries criterion that was set for the **radius-server dead-criteria** command.

```
Router (config)# no radius-server dead-criteria tries 4
```

Related Commands

Command	Description
debug aaa dead-criteria transactions	Displays AAA dead-criteria transaction values.
show aaa dead-criteria	Displays dead-criteria information for a AAA server.
show aaa server-private	Displays the status of all private RADIUS servers.
show aaa servers	Displays information about the number of packets sent to and received from AAA servers.

radius-server deadtime

To improve RADIUS response time when some servers might be unavailable and to skip unavailable servers immediately, use the **radius-server deadtime** command in global configuration mode. To set dead time to 0, use the **no** form of this command.

radius-server deadtime *minutes*

no radius-server deadtime

Syntax Description

minutes	Length of time, in minutes (up to a maximum of 1440 minutes or 24 hours), for which a RADIUS server is skipped over by transaction requests.

Command Default

Dead time is set to 0.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to enable the Cisco IOS software to mark as "dead" any RADIUS servers that fail to respond to authentication requests, thus avoiding the wait for the request to time out before trying the next configured server. A RADIUS server marked as "dead" is skipped by additional requests for the specified duration (in minutes) or unless there are no servers not marked as "dead."

Note If a RADIUS server that is marked as "dead" receives a directed-request, the directed- request is not omitted by the RADIUS server. The RADIUS server continues to process the directed-request because the request is directly sent to the RADIUS server.

When the RADIUS Server Is Marked As Dead

For Cisco IOS versions prior to 12.2(13.7)T, the RADIUS server will be marked as dead if a packet is transmitted for the configured number of retransmits and a valid response is not received from the server within the configured timeout for any of the RADIUS packet transmissions.

For Cisco IOS versions 12.2(13.7)T and later, the RADIUS server will be marked as dead if both of the following conditions are met:

1. A valid response has not been received from the RADIUS server for any outstanding transaction for at least the timeout period that is used to determine whether to retransmit to that server, and

2. At at least the requisite number of retransmits plus one (for the initial transmission) have been sent consecutively across all transactions being sent to the RADIUS server without receiving a valid response from the server within the requisite timeout.

Examples

The following example specifies five minutes of dead time for RADIUS servers that fail to respond to authentication requests:

```
radius-server deadtime 5
```

Related Commands

Command	Description
deadtime (server-group configuration)	Configures deadtime within the context of RADIUS server groups.
radius-server host	Specifies a RADIUS server host.
radius-server retransmit	Specifies the number of times that the Cisco IOS software searches the list of RADIUS server hosts before giving up.
radius-server timeout	Sets the interval for which a router waits for a server host to reply.

radius-server directed-request

To allow users to log in to a Cisco Network Access Server (NAS) and select a RADIUS server for authentication, use the **radius-server directed-request** command in global configuration mode. To disable the directed-request function, use the **no** form of this command.

radius-server directed-request [**restricted**]

no radius-server directed-request [**restricted**]

Syntax Description

restricted	(Optional) Prevents the user from being sent to a secondary server if the specified server is not available.

Command Default

The User cannot log in to a Cisco NAS and select a RADIUS server for authentication.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is integrated into Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **radius-server directed-request** command sends only the portion of the username before the "@" symbol to the host specified after the "@" symbol. In other words, with this command enabled, you can direct a request to any of the configured servers, and only the username is sent to the specified server.

Note If a private RADIUS server is used as the group server by configuring the **server-private** (RADIUS) command, then the **radius-server directed-request** command cannot be configured.

The following is the sequence of events to send a message to RADIUS servers:

- If the **radius-server directed-request** command is configured:
  - A request is sent to the directed server. If there are more servers with the same IP address, the request is sent only to the first server with same IP address.
  - If a response is not received, requests will be sent to all servers listed in the first method list.
  - If no response is received with the first method, the request is sent to all servers listed in the second method list until the end of the method list is reached.

Note To select the directed server, search the first server group in the method list for a server with the IP address provided in a directed request. If it is not available, the first server group with the same IP address from the global pool is considered.

- If the **radius-server directed-request restricted** command is configured for every server group in the method list, until the response is received from the directed server or the end of method list is reached, the following actions occur:
  - The first server with an IP address of the directed server will be used to send the request.
  - If a server with the same IP address is not found in the server group, then the first server in the global pool with the IP address of the directed-server will be used.

If the **radius-server directed-request** command is disabled using the **no radius-server directed-request** command, the entire string, both before and after the "@" symbol, is sent to the default RADIUS server. The router queries the list of servers, starting with the first one in the list. It sends the whole string, and accepts the first response from the server.

Use the **radius-server directed-request restricted** command to limit the user to the RADIUS server identified as part of the username.

If the user request has a server IP address, then the directed server forwards it to a specific server before forwarding it to the group. For example, if a user request such as user@10.0.0.1 is sent to the directed server, and if the IP address specified in this user request is the IP address of a server, the directed server forwards the user request to the specific server.

If a directed server is configured both on the server group and on the host server, and if the user request with the configured server name is sent to the directed server, the directed server forwards the user request to the host server before forwarding it to the server group. For example, if a user request of user@10.0.0.1 is sent to the directed server and 10.0.0.1 is the host server address, then the directed server forwards the user request to the host server before forwarding the request to the server group.

Note When the **no radius-server directed-request restricted** command is entered, only the restricted flag is removed, and the directed-request flag is retained. To disable the directed-request function, you must also enter the **no radius-server directed-request** command.

Examples

The following example shows how to verify that the RADIUS server is selected based on the directed request:

```
aaa new-model
aaa authentication login default radius
radius-server host 192.168.1.1
radius-server host 172.16.56.103
radius-server host 172.31.40.1
radius-server directed-request
```

Related Commands

Command	Description
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.

Command	Description
radius-server host	Specifies a RADIUS server host.
server-private (RADIUS)	Configures the IP address of the private RADIUS server for the group server.

radius-server domain-stripping

To configure a network access server (NAS) to strip suffixes, or to strip both suffixes and prefixes from the username before forwarding the username to the remote RADIUS server, use the **radius-server domain-stripping** command in global configuration mode. To disable a stripping configuration, use the **no** form of this command.

Note The **ip vrf default** command must be configured in global configuration mode before the **radius-server domain-stripping** command is configured to ensure that the default VRF name is a NULL value until the defaulf vrf name is configured.

radius-server domain-stripping [[**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] | **strip-suffix** *suffix*] [**vrf** *vrf-name*]

no radius-server domain-stripping [[**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] | **strip-suffix** *suffix*] [**vrf** *vrf-name*]

Syntax Description

right-to-left	(Optional) Specifies that the NAS will apply the stripping configuration at the first delimiter found when parsing the full username from right to left. The default is for the NAS to apply the stripping configuration at the first delimiter found when parsing the full username from left to right.
prefix-delimiter *character* [*character2...character7*]	(Optional) Enables prefix stripping and specifies the character or characters that will be recognized as a prefix delimiter. Valid values for the *character* argument are @, /, $, %, \, #, and -. Multiple characters can be entered without intervening spaces. Up to seven characters can be defined as prefix delimiters, which is the maximum number of valid characters. If a \ is entered as the final or only value for the *character* argument, it must be entered as \\. No prefix delimiter is defined by default.
delimiter *character* [*character2...character7*]	(Optional) Specifies the character or characters that will be recognized as a suffix delimiter. Valid values for the *character* argument are @, /, $, %, \, #, and -. Multiple characters can be entered without intervening spaces. Up to seven characters can be defined as suffix delimiters, which is the maximum number of valid characters. If a \ is entered as the final or only value for the *character* argument, it must be entered as \\. The default suffix delimiter is the @ character.
strip-suffix *suffix*	(Optional) Specifies a suffix to strip from the username.
vrf *vrf-name*	(Optional) Restricts the domain stripping configuration to a Virtual Private Network (VPN) routing and forwarding (VRF) instance. The *vrf-name* argument specifies the name of a VRF.

Command Default

Stripping is disabled. The full username is sent to the RADIUS server.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)DD	This command was introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(4)T	Support was added for the **right-to-left** and **delimiter** *character* keywords and argument.
12.4(4)T	Support was added for the **strip-suffix** *suffix* and **prefix-delimiter** keywords and argument.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.(33)SRC.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
XE 2.1	This command was integrated into Cisco IOS Release XE 2.1.
XE 2.5	Support was added for the **strip-suffix** *suffix* and **prefix-delimiter** keywords and argument.

Usage Guidelines

Use the **radius-server domain-stripping** command to configure the NAS to strip the domain from a username before forwarding the username to the RADIUS server. If the full username is user1@cisco.com, enabling the **radius-server domain-stripping** command results in the username "user1" being forwarded to the RADIUS server.

Use the **right-to-left** keyword to specify that the username should be parsed for a delimiter from right to left, rather than from left to right. This allows strings with two instances of a delimiter to strip the username at either delimiter. For example, if the username is user@cisco.com@cisco.net, the suffix could be stripped in two ways. The default direction (left to right) would result in the username "user" being forwarded to the RADIUS server. Configuring the **right-to-left** keyword would result in the username "user@cisco.com" being forwarded to the RADIUS server.

Use the **prefix-delimiter** keyword to enable prefix stripping and to specify the character or characters that will be recognized as a prefix delimiter. The first configured character that is parsed will be used as the prefix delimiter, and any characters before that delimiter will be stripped.

Use the **delimiter** keyword to specify the character or characters that will be recognized as a suffix delimiter. The first configured character that is parsed will be used as the suffix delimiter, and any characters after that delimiter will be stripped.

Use **strip-suffix** *suffix* to specify a particular suffix to strip from usernames. For example, configuring the **radius-server domain-stripping strip-suffix cisco.net** command would result in the username user@cisco.net being stripped, while the username user@cisco.com will not be stripped. You may configure multiple suffixes for stripping by issuing multiple instances of the **radius-server domain-stripping** command. The default suffix delimiter is the @ character.

Note Issuing the **radius-server domain-stripping strip-suffix** *suffix* command disables the capacity to strip suffixes from all domains. Both the suffix delimiter and the suffix must match for the suffix to be stripped from the full username. The default suffix delimiter of @ will be used if you do not specify a different suffix delimiter or set of suffix delimiters using the **delimiter** keyword.

To apply a domain-stripping configuration only to a specified VRF, use the **vrf** *vrf-name* option.

The interactions between the different types of domain stripping configurations are as follows:

- You may configure only one instance of the **radius-server domain-stripping** [**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] command.
- You may configure multiple instances of the **radius-server domain-stripping** [**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] [**vrf** *vrf-name*] command with unique values for **vrf** *vrf-name*.
- You may configure multiple instances of the **radius-server domain-stripping strip-suffix** *suffix* [**vrf** *per-vrf*] command to specify multiple suffixes to be stripped as part of a global or per-VRF ruleset.
- Issuing any version of the **radius-server domain-stripping** command automatically enables suffix stripping using the default delimiter character @ for that ruleset, unless a different delimiter or set of delimiters is specified.
- Configuring a per-suffix stripping rule disables generic suffix stripping for that ruleset. Only suffixes that match the configured suffix or suffixes will be stripped from usernames.

Examples

The following example configures the router to parse the username from right to left and sets the valid suffix delimiter characters as @, \, and $. If the full username is cisco/user@cisco.com$cisco.net, the username “cisco/user@cisco.com” will be forwarded to the RADIUS server because the $ character is the first valid delimiter encountered by the NAS when parsing the username from right to left.

```
radius-server domain-stripping right-to-left delimiter @\$
```

The following example configures the router to strip the domain name from usernames only for users associated with the VRF instance named abc. The default suffix delimiter @ will be used for generic suffix stripping.

```
radius-server domain-stripping vrf abc
```

The following example enables prefix stripping using the character / as the prefix delimiter. The default suffix delimiter character @ will be used for generic suffix stripping. If the full username is cisco/user@cisco.com, the username “user” will be forwarded to the RADIUS server.

```
radius-server domain-stripping prefix-delimiter /
```

The following example enables prefix stripping, specifies the character / as the prefix delimiter, and specifies the character # as the suffix delimiter. If the full username is cisco/user@cisco.com#cisco.net, the username “user@cisco.com” will be forwarded to the RADIUS server.

```
radius-server domain-stripping prefix-delimiter / delimiter #
```

The following example enables prefix stripping, configures the character / as the prefix delimiter, configures the characters $, @, and # as suffix delimiters, and configures per-suffix stripping of the suffix cisco.com. If the full username is cisco/user@cisco.com, the username “user” will be forwarded to the RADIUS server. If the full username is cisco/user@cisco.com#cisco.com, the username “user@cisco.com” will be forwarded.

```
radius-server domain-stripping prefix-delimiter / delimiter $@#
radius-server domain-stripping strip-suffix cisco.com
```

The following example configures the router to parse the username from right to left and enables suffix stripping for usernames with the suffix cisco.com. If the full username is cisco/user@cisco.net@cisco.com, the username "cisco/user@cisco.net" will be forwarded to the RADIUS server. If the full username is cisco/user@cisco.com@cisco.net, the full username will be forwarded.

```
radius-server domain-stripping right-to-left
radius-server domain-stripping strip-suffix cisco.com
```

The following example configures a set of global stripping rules that will strip the suffix cisco.com using the delimiter @, and a different set of stripping rules for usernames associated with the VRF named myvrf:

```
radius-server domain-stripping strip-suffix cisco.com
!
radius-server domain-stripping prefix-delimiter # vrf myvrf
radius-server domain-stripping strip-suffix cisco.net vrf myvrf
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
ip vrf	Defines a VRF instance and enters VRF configuration mode.
tacacs-server domain-stripping	Configures a router to strip a prefix or suffix from the username before forwarding the username to the TACACS+ server.

radius-server extended-portnames

The **radius-server extended-portnames** command is replaced by the **radius-server attribute nas-port format** command. See the description of the **radius-server attribute nas-port format** command for more information.

radius-server host

To specify a RADIUS server host, use the **radius-server host** command in global configuration mode. To delete the specified RADIUS host, use the **no** form of this command.

Cisco IOS Releases 12.2SB and 12.2SR

radius-server host {*hostname* | *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*] [**ignore-auth-port**] [**acct-port** *port-number*] [**ignore-acct-port**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] [**idle-time** *minutes*] [**backoff exponential** {**backoff-retry** *number-of-retransmits* | **max-delay** *minutes*}] [**key** *encryption-key*]

no radius-server host {*hostname* | *ip-address*}

All Other Releases

radius-server host {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] [**backoff exponential** {**backoff-retry** *number-of-retransmits* | **max-delay** *minutes*}] [**pac** [**key** *encryption-key*] | **key** *encryption-key*]

no radius-server host {*hostname* | *ip-address*}

Syntax Description

hostname	Domain Name System (DNS) name of the RADIUS server host.
ip-address	IP address of the RADIUS server host.
test username	(Optional) Turns on the automated testing feature for RADIUS server load balancing.
user-name	(Optional) Test user ID username.
auth-port	(Optional) Specifies the User Datagram Protocol (UDP) destination port for authentication requests.
port-number	(Optional) The port number for authentication requests; the host is not used for authentication if the port number is set to 0. If the port number is not specified, the port number defaults to 1645.
ignore-auth-port	(Optional) Turns off the automated testing feature for RADIUS server load balancing on the authentication port.
acct-port	(Optional) Specifies the UDP destination port for accounting requests.
ignore-acct-port	(Optional) Turns off the automated testing feature for RADIUS server load balancing on the accounting port.
timeout *seconds*	(Optional) Specifies the time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the **radius-server timeout** command. If no timeout value is specified, the global value is used. Enter a value in the range 1 to 1000.
retransmit *retries*	(Optional) Specifies the number of times a RADIUS request is re-sent to a server, if that server is not responding or is responding slowly. This setting overrides the global setting of the **radius-server retransmit** command. If no retransmit value is specified, the global value is used. Enter a value in the range 1 to 100.

key	(Optional) Specifies the authentication and encryption key used between the router and the RADIUS daemon running on this RADIUS server. This key overrides the global setting of the **radius-server key** command. If no key string is specified, the global value is used. The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command syntax. This is because the leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.
string	(Optional) Authentication and encryption key for all RADIUS communications between the router and the RADIUS server. This key must match the encryption used on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.
alias	(Optional) Allows up to eight aliases per line for any given RADIUS server.
idle-time *minutes*	(Optional) Specifies the length of time the server remains idle before it is quarantined and test packets are sent out. • Default is 60 minutes (1 hour). • The valid range is 1 to 35791 seconds.
backoff exponential	(Optional) Specifies the exponential retransmits backup mode.
backoff-retry *number-of-retransmits*	Specifies the exponential backoff retry. • *number-of-retransmits*—Number of backoff retries. Value = 1 through 50. The default is 8.
max-delay *minutes*	Specifies the maximum delay between retransmits. • *minutes*—Value = 1 through 120 minutes. The default is 3 minutes.
pac	(Optional) Specifies that automatic Protected Access Credential (PAC) provisioning is triggered. **Note** The **pac** keyword is mutually exclusive with the shared secret **key** keyword that already exists.
key *encryption-key*	Specifies the per-server encryption key (overrides the default). • *encryption-key*—Can be **0** (specifies that an unencrypted keys follows), **7** (specifies that a hidden key follows), or a line specifying the unencrypted (clear-text) server key.

Defaults

No RADIUS host is specified; use global **radius-server** command values.

RADIUS server load balancing automated testing is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.0(5)T	This command was modified to add options for configuring timeout, retransmission, and key values per RADIUS server.
12.1(3)T	The **alias** keyword was added on the Cisco AS5300 and AS5800 universal access servers.
12.2(15)B	The **backoff exponential**, **backoff-retry**, **key**, and **max-delay** keywords and *number-of-retransmits, encryption-key*, and *minutes* arguments were added.
12.2(28)SB	The **test username** *user-name*, **ignore-auth-port**, **ignore-acct-port**, and **idle-time** *seconds* keywords and arguments were added for configuring RADIUS server load balancing automated testing functionality. **Note** The keywords and arguments added in Cisco IOS Release 12.2(28)SB apply to any subsequent 12.2SB releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. The keywords and arguments that were added in Cisco IOS Release 12.2(28)SB apply to Cisco IOS Release 12.2(33)SRA and subsequent 12.2SR releases.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T. **Note** The keywords and arguments that were added in Cisco IOS Release 12.2(28)SB do not apply to Cisco IOS Release 12.4(11)T or to subsequent 12.4T releases.
12.2 SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. **Note** The keywords and arguments that were added in Cisco IOS Release 12.2(28)SB do not apply to Cisco IOS Release 12.2SX.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

You can use multiple **radius-server host** commands to specify multiple hosts. The software searches for hosts in the order in which you specify them.

You can specify the keywords of the **radius-server host** command in any order. However, the **pac** keyword always precedes the **key** *encryption-key* keyword.

If you do not specify the port number for authentication requests for both the **acct-port** and the **auth-port** keywords, the port number defaults to 1645.

If no host-specific timeout, retransmit, or key values are specified, the global values apply to each host.

We recommend the use of a test user who is not defined on the RADIUS server for the automated testing of the RADIUS server. This is to protect against security issues that can arise if the test user is not configured correctly.

If you configure one RADIUS server with the nonstandard option and another RADIUS server without the nonstandard option, the RADIUS-server host with the nonstandard option does not accept a predefined host. If you configure the same RADIUS server host IP address for a different UDP destination port for accounting requests using the **acct-port** keyword and a UDP destination port for authentication requests using the **auth-port** keyword with and without the nonstandard option, the RADIUS server does not accept the nonstandard option.

Because entering a line resets all the port numbers, you must specify a host and configure accounting and authentication ports on a single line.

To use separate servers for accounting and authentication, use the zero port value as appropriate.

RADIUS Server Automated Testing (for Cisco IOS Release 12.2(28)SB)

When you use the **radius-server host** command to enable automated testing for RADIUS server load balancing:

- The authentication port is enabled by default. If the port number is not specified, the default port of 1645 is used. To disable the authentication port, specify the **ignore-auth-port** keyword.
- The accounting port is enabled by default. If the port number is not specified, the default port of 1645 is used. To disable the accounting port, specify the **ignore-acct-port** keyword.

Examples

Releases Other than Cisco IOS Release 12.2(28)SB

The following example specifies *host1* as the RADIUS server and uses default ports for both accounting and authentication:

```
radius-server host host1
```

The following example specifies port 1612 as the destination port for authentication requests and port 1616 as the destination port for accounting requests on the RADIUS host named host1:

```
radius-server host host1 auth-port 1612 acct-port 1616
```

Because entering a line resets all the port numbers, you must specify a host and configure accounting and authentication ports on a single line.

The following example specifies the host with IP address 192.0.2.46 as the RADIUS server, uses ports 1612 and 1616 as the authorization and accounting ports, sets the timeout value to 6, sets the retransmit value to 5, and sets “rad123” as the encryption key, matching the key on the RADIUS server:

```
radius-server host 192.0.2.46 auth-port 1612 acct-port 1616 timeout 6 retransmit 5 key
rad123
```

To use separate servers for accounting and authentication, use the zero port value as appropriate.

The following example specifies that RADIUS server host1 be used for accounting but not for authentication, and that RADIUS server host2 be used for authentication but not for accounting:

```
radius-server host host1.example.com auth-port 0
radius-server host host2.example.com acct-port 0
```

The following example specifies four aliases on the RADIUS server with IP address 192.0.2.1:

```
radius-server host 192.0.2.1 auth-port 1646 acct-port 1645
radius-server host 192.0.2.1 alias 192.0.2.2 192.0.2.3 192.0.2.4
```

The following example shows how to enable exponential backoff retransmits on a per-server basis. In this example, assume that the retransmit is configured for three retries and the timeout is configured for 5 seconds; that is, the RADIUS request will be transmitted three times with a delay of 5 seconds. Thereafter, the router will continue to retransmit RADIUS requests with a delayed interval that doubles each time until 32 retries have been achieved. The router will stop doubling the retransmit intervals after the interval surpasses the configured 60 minutes; it will transmit every 60 minutes.

The **pac** keyword allows the PAC-Opaque, which is a variable length field, to be sent to the server during the Transport Layer Security (TLS) tunnel establishment phase. The PAC-Opaque can be interpreted only by the server to recover the required information for the server to validate the peer's identity and authentication. For example, the PAC-Opaque may include the PAC-Key and the PAC's peer identity. The PAC-Opaque format and contents are specific to the issuing PAC server.

The following example configures automatic PAC provisioning on a router. In seed devices, also known as core switches, the PAC-Opaque has to be provisioned so that all RADIUS exchanges can use this PAC-Opaque to enable automatic PAC provisioning for the server being used. All nonseed devices obtain the PAC-Opaque during the authentication phase of a link initialization.

```
enable
configure terminal
radius-server host 10.0.0.1 auth-port 1812 acct-port 1813 pac
```

Cisco IOS Release 12.2(28)SB

The following example shows how to enable RADIUS server automated testing for load balancing with the authorization and accounting ports specified:

```
radius-server host 192.0.2.176 test username test1 auth-port 1645 acct-port 1646
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication ppp	Specifies one or more AAA authentication method for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict network access to a user.
debug aaa test	Shows when the idle timer or dead timer has expired for RADIUS server load balancing.
load-balance	Enables RADIUS server load balancing for named RADIUS server groups.
ppp	Starts an asynchronous connection using PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
radius-server load-balance	Enables RADIUS server load balancing for the global RADIUS server group.
radius-server retransmit	Specifies how many times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
radius-server timeout	Sets the interval a router waits for a server host to reply.
test aaa group	Tests RADIUS load balancing server response manually.
username	Establishes a username-based authentication system, such as PPP CHAP and PAP.

radius-server host non-standard

To identify that the security server is using a vendor-proprietary implementation of RADIUS, use the **radius-server host non-standard** command in global configuration mode. This command tells the Cisco IOS software to support nonstandard RADIUS attributes. To delete the specified vendor-proprietary RADIUS host, use the **no** form of this command.

radius-server host {*host-name* | *ip-address*} **non-standard**

no radius-server host {*host-name* | *ip-address*} **non-standard**

Syntax Description

host-name	DNS name of the RADIUS server host.
ip-address	IP address of the RADIUS server host.

Defaults

No RADIUS host is specified.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **radius-server host non-standard** command enables you to identify that the RADIUS server is using a vendor-proprietary implementation of RADIUS. Although an IETF draft standard for RADIUS specifies a method for communicating information between the network access server and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. This command enables the Cisco IOS software to support the most common vendor-proprietary RADIUS attributes. Vendor-proprietary attributes will not be supported unless you use the **radius-server host non-standard** command.

For a list of supported vendor-specific RADIUS attributes, refer to the appendix "RADIUS Attributes" in the *Cisco IOS Security Configuration Guide*.

Examples

The following example specifies a vendor-proprietary RADIUS server host named *alcatraz*:

```
radius-server host alcatraz non-standard
```

Related Commands

Command	Description
radius-server configure-nas	Allows the Cisco router or access server to query the vendor-proprietary RADIUS server for the static routes and IP pool definitions used throughout its domain when the device starts up.
radius-server host	Specifies a RADIUS server host.

radius-server key

To set the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon, use the **radius-server key** command in global configuration mode. To disable the key, use the **no** form of this command.

radius-server key {***0*** *string* | ***7*** *string*} *string*

no radius-server key

Syntax Description

0	Specifies that an unencrypted key will follow.
string	The unencrypted (cleartext) shared key.
7	Specifies that a hidden key will follow.
string	The hidden shared key.
string	The unencrypted (cleartext) shared key.

Command Default

The authentication and encryption key is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.1(3)T	This command was modified. The *string* argument was modified as follows: • **0** *string* • **7** *string* • *string*
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

After enabling authentication, authorization, and accounting (AAA) authentication with the **aaa new-model** command, you must set the authentication and encryption key using the **radius-server key** command.

Note Specify a RADIUS key after you issue the **aaa new-model** command.

The key entered must match the key used on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

Examples

The following example sets the authentication and encryption key to “key1”:

```
Router(config)# radius-server key key1
```

The following example sets the authentication and encryption key to “anykey.” The 7 specifies that a hidden key will follow.

```
service password-encryption
radius-server key 7 anykey
```

After you save your configuration and use the **show-running config** command, an encrypted key will be displayed as follows:

```
Router# show running-config
!
!
 radius-server key 7 19283103834782sda
! The leading 7 indicates that the following text is encrypted.
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.
aaa new-model	Enables AAA access control model.
ppp	Starts an asynchronous connection using PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
radius-server host	Specifies a RADIUS server host.
service password-encryption	Encrypt passwords.
username	Establishes a username-based authentication system, such as PPP CHAP and PAP.

radius-server load-balance

To enable RADIUS server load balancing for the global RADIUS server group referred to as "radius" in the authentication, authorization and accounting (AAA) method lists, use the **radius-server load-balance** command in global configuration mode. To disable RADIUS server load balancing, use the **no** form of this command.

radius-server load-balance method least-outstanding [**batch-size** *number*] [**ignore-preferred-server**]

no radius-server load-balance

Syntax Description

method least-outstanding	Enables least outstanding mode for load balancing.
batch-size	(Optional) The number of transactions to be assigned per batch.
number	(Optional) The number of transactions in a batch. • The default is 25. • The range is 1–2147483647. **Note** Batch size may impact throughput and CPU load. It is recommended that the default batch size, 25, be used because it is optimal for high throughput, without adversely impacting CPU load.
ignore-preferred-server	(Optional) Indicates if a transaction associated with a single AAA session should attempt to use the same server or not. • If set, preferred server setting will not be used. • Default is to use the preferred server.

Command Defaults

If this command is not configured, global RADIUS server load balancing will not occur.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Examples

The following example shows how to enable load balancing for global RADIUS server groups. It is shown in three parts: the current configuration of RADIUS command output, debug output, and AAA server status information. You can use the delimiting characters to display only the relevant parts of the configuration.

Server Configuration and Enabling Load Balancing for Global RADIUS Server Group Example

The following shows the relevant RADIUS configuration:

```
Router# show running-config | inc radius

aaa authentication ppp default group radius
aaa accounting network default start-stop group radius
radius-server host 192.0.2.238 auth-port 2095 acct-port 2096 key cisco
radius-server host 192.0.2.238 auth-port 2015 acct-port 2016 key cisco
radius-server load-balance method least-outstanding batch-size 5
```

The lines in the current configuration of RADIUS command output above are defined as follows:

- The **aaa authentication ppp** command authenticates all PPP users using RADIUS.
- The **aaa accounting** command enables the sending of all accounting requests to the AAA server after the client is authenticated and after the disconnect using the keyword start-stop.
- The **radius-server host** command defines the IP address of the RADIUS server host with the authorization and accounting ports specified and the authentication and encryption key identified.
- The **radius-server load-balance** command enables load balancing for the global RADIUS server groups with the batch size specified.

Debug Output for Global RADIUS Server Group Example

The debug output below shows the selection of preferred server and processing of requests for the configuration above.

```
Router# show debug

General OS:
  AAA server group server selection debugging is on
Router#
<sending 10 pppoe requests>
Router#
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000014):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[0] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Selected Server[0] with load 0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000014):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000015):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000015):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000016):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000016):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000017):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
```

```
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000017):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000018):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000018):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000019):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[0] load:5
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Selected Server[1] with load 0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000019):Server (192.0.2.238:2015,2016) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(0000001A):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT(0000001A):Server (192.0.2.238:2015,2016) now
being used as preferred server
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT(0000001B):No preferred server available.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT(0000001B):Server (192.0.2.238:2015,2016) now
being used as preferred server
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT(0000001C):No preferred server available.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT(0000001C):Server (192.0.2.238:2015,2016) now
being used as preferred server
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT(0000001D):No preferred server available.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server
.
.
.
```

Server Status Information for Global RADIUS Server Group Example

The output below shows the AAA server status for the global RADIUS server group configuration example.

```
Router# show aaa server

RADIUS:id 4, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
     State:current UP, duration 3175s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 6, timeouts 1
             Response:unexpected 1, server error 0, incorrect 0, time 1841ms
             Transaction:success 5, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 5, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 3303ms
```

```
            Transaction:success 5, failure 0
     Elapsed time since counters last cleared:2m

RADIUS:id 5, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
     State:current UP, duration 3175s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 6, timeouts 1
            Response:unexpected 1, server error 0, incorrect 0, time 1955ms
            Transaction:success 5, failure 0
     Author:request 0, timeouts 0
            Response:unexpected 0, server error 0, incorrect 0, time 0ms
            Transaction:success 0, failure 0
     Account:request 5, timeouts 0
            Response:unexpected 0, server error 0, incorrect 0, time 3247ms
            Transaction:success 5, failure 0
     Elapsed time since counters last cleared:2m
Router#
```

The output shows the status of two RADIUS servers. Both servers are up and, in the last 2 minutes, have processed successfully:

- 5 out of 6 authentication requests
- 5 out of 5 accounting requests

Related Commands

Command	Description
debug aaa sg-server selection	Shows why the RADIUS and TACACS+ server group system in a router is selecting a particular server.
debug aaa test	Shows when the idle timer or dead timer has expired for RADIUS server load balancing.
load-balance	Enables RADIUS server load balancing for named RADIUS server groups.
radius-server host	Enables RADIUS automated testing for load balancing.
test aaa group	Tests RADIUS load balancing server response manually.

radius-server local

To enable the access point or wireless-aware router as a local authentication server and to enter into configuration mode for the authenticator, use the **radius-server local** command in global configuration mode. To remove the local RADIUS server configuration from the router or access point, use the **no** form of this command.

radius-server local

no radius-server local

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows that the access point is being configured to serve as a local authentication server:

```
Router(config)# radius-server local
```

Usage Guidelines

This command is not supported on bridges.

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.

Command	Description
debug -server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

radius local-server pac-generate expiry

To configure the expiry and password encryption for the Protected Access Credentials (PAC) in the RADIUS local server, use the **radius local-server pac-generate expiry** command in privileged EXEC mode.

radius local-server pac-generate expiry *filename* [**password** *string*] [**expiry** *days*]

Syntax Description

filename	Filename to save the generated PAC.
password *string*	(Optional) Specifies to encrypt the PAC password and the password to be encrypted.
expiry *days*	(Optional) Specifies to encrypt the expiry time of the generated PAC and the number of days. The range is from 1 to 4095. Default is one day.

Command Default

The expiry encryption for PAC in the RADIUS local server is one day.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to configure the router to expire the “user.pac” file in two days:

```
Router# radius local-server pac-generate expiry user.pac expiry 2
```

Related Commands

Command	Description
show radius local-server statistics	Displays the statistics for the local authentication server.

radius-server optional-passwords

To specify that the first RADIUS request to a RADIUS server be made *without* password verification, use the **radius-server optional-passwords** command in global configuration mode. To restore the default, use the **no** form of this command.

radius-server optional-passwords

no radius-server optional-passwords

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the user enters the login name, the login request is transmitted with the name and a zero-length password. If accepted, the login procedure completes. If the RADIUS server refuses this request, the server software prompts for a password and tries again when the user supplies a password. The RADIUS server must support authentication for users without passwords to make use of this feature.

Examples

The following example configures the first login to not require RADIUS verification:

```
radius-server optional-passwords
```

radius-server retransmit

To specify the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up, use the **radius-server retransmit** command in global configuration mode. To disable retransmission, use the **no** form of this command.

radius-server retransmit *retries*

no radius-server retransmit

Syntax Description

retries	Maximum number of retransmission attempts. The range is 0 to 100.

Command Default

The default number of retransmission attempts is 3.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

The Cisco IOS software tries all servers, allowing each one to time out before increasing the retransmit count.

If the RADIUS server is only a few hops from the router, we recommend that you configure the RADIUS server retransmit rate to 5.

Examples

The following example shows how to specify a retransmit counter value of five times:

```
Router(config)# radius-server retransmit 5
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.

Command	Description
radius-server timeout	Sets the interval for which a router waits for a server host to reply.
show radius statistics	Displays the RADIUS statistics for accounting and authentication packets.

radius-server retry method reorder

To specify the reordering of RADIUS traffic retries among a server group, use the **radius-server retry method reorder** command in global configuration mode. To disable the reordering of retries among the server group, use the **no** form of this command.

radius-server retry method reorder

no radius-server retry method reorder

Syntax Description

This command has no arguments or keywords.

Defaults

If this command is not configured, RADIUS traffic is not reordered among the server group.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Use this command to reorder RADIUS traffic to another server in the server group when the first server fails in periods of high load. Subsequent to the failure, all RADIUS traffic is directed to the new server. Traffic is switched from the new server to another server in the server group only if the new server also fails. Traffic will not be automatically switched back to the first server.

If the **radius-server retry method reorder** command is not configured, each RADIUS server is used until marked dead. The nondead server that is closest to the beginning of the list is used for the first transmission of a transaction and for the configured number of retransmissions. Each nondead server in the list is thereafter tried in turn.

Examples

The following example shows that RADIUS server retry has been configured:

```
aaa new-model
radius-server retry method reorder
radius-server retransmit 0
radius-server transaction max-tries 6
radius-server host 192.2.3.4 key rad123
radius-server host 192.5.6.7 key rad123
```

Related Commands

Command	Description
radius-server transaction max-tries	Specifies the maximum number of transmissions that may be retried per transaction on a RADIUS server.

radius-server source-ports extended

To enable 200 ports in the range from 21645 to 21844 to be used as the source ports for sending out RADIUS requests, use the **radius-server source-ports extended** command in global configuration mode. To return to the default setting, in which ports 1645 and 1646 are used as the source ports for RADIUS requests, use the **no** form of this command.

radius-server source-ports extended

no radius-server source-ports extended

Syntax Description

This command has no arguments or keywords.

Defaults

Ports 1645 and 1646 are used as the source ports for RADIUS requests.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

The identifier field of the RADIUS packet is 8 bits long, and yields 256 unique identifiers. A NAS uses one port (1645) as the source port to send out access requests to the RADIUS server and one port (1646) as the source port to send out accounting requests to the RADIUS server. This scheme allows for 256 outstanding access requests and 256 outstanding accounting requests.

If the number of outstanding access requests or accounting requests exceeds 256, the port and ID space will wrap, and all subsequent RADIUS requests will be forced to reuse ports and IDs that are already in use. When the RADIUS server receives a request that uses a port and ID that is already in use, it treats the request as a duplicate. The RADIUS server then drops the request.

The **radius-server source-ports extended** command allows you to configure the NAS to use 200 ports in the range from 21645 to 21844 as the source ports for sending out RADIUS requests. Having 200 source ports allows up to 256*200 authentication and accounting requests to be outstanding at one time. During peak call volume, typically when a router first boots or when an interface flaps, the extra source ports allow sessions to recover more quickly on large-scale aggregation platforms.

Examples

The following example shows how to configure a NAS to use 200 ports in the range from 21645 to 21844 as the source ports for RADIUS requests:

```
Router(config)# radius-server source-ports extended
```

radius-server throttle

To configure throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server, use the **radius-server throttle** command in global configuration mode. To disable throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server, use the **no** form of this command.

radius-server throttle {[**accounting** *threshold*] [**access** *threshold* [**access-timeout** *number-of-timeouts*]]}

no radius-server throttle {[**accounting** *threshold*] [**access** *threshold* [**access-timeout** *number-of-timeouts*]]}

Syntax Description

accounting *threshold*	Configures the threshold value for accounting requests sent to a RADIUS server. The range is 0 through 65536. The default value is 0 (throttling disabled).
access *threshold*	Configures the threshold value for access requests sent to a RADIUS server. The range is 0 through 65536. The default value is 0 (throttling disabled).
access-timeout *number-of-timeouts*	(Optional) Specifies the number of consecutive access timeouts that are allowed before the access request is dropped. The range is 1 through 10. The default value is 3.

Command Default

Throttling is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was implemented on the Cisco 10,000 series routers.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to configure throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server.

Examples

The following examples show how to configure throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server.

The following example shows how to limit the number of accounting requests sent to a RADIUS server to 100:

```
Router> enable
Router# configure terminal
Router(config)# radius-server throttle accounting 100
```

The following example shows how to limit the number of access request packets sent to a RADIUS server to 200 and sets the number of timeouts allowed per transactions to 2:

```
Router> enable
Router# configure terminal
Router(config)# radius-server throttle access 200
Router(config)# radius-server throttle access 200 access-timeout 2
```

The following example shows how to throttle both accounting and access request packets:

```
Router> enable
Router# configure terminal
Router(config)# radius-server throttle accounting 100 access 200
```

Related Commands

Command	Description
radius-server host	Specifies a RADIUS server host.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
radius-server retransmit	Specifies the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
radius-server timeout	Specifies the number of seconds a router waits for a server host to reply before timing out.
show radius statistics	Displays the RADIUS statistics for accounting and authentication packets.
throttle	Configures server group throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server.

radius-server timeout

To set the interval for which a router waits for a server host to reply, use the **radius-server timeout** command in global configuration mode. To restore the default, use the **no** form of this command.

radius-server timeout *seconds*

no radius-server timeout

Syntax Description

seconds	Number that specifies the timeout interval, in seconds. The range is 1 to 1000. The default is 5 seconds.

Defaults

5 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to set the number of seconds a router waits for a server host to reply before timing out.

If the RADIUS server is only a few hops from the router, we recommend that you configure the RADIUS server timeout to 15 seconds.

Examples

The following example shows how to set the interval timer to 10 seconds:

```
radius-server timeout 10
```

Related Commands

Command	Description
radius-server host	Specifies a RADIUS server host.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
radius-server retransmit	Specifies the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
show radius statistics	Displays the RADIUS statistics for accounting and authentication packets.

radius-server transaction max-tries

To specify the maximum number of transmissions that may be retried per transaction on a RADIUS server, use the **radius-server transaction max-retries** command in global configuration mode. To disable the number of retries that were configured, use the **no** form of this command.

radius-server transaction max-tries *number*

no radius-server transaction max-tries *number*

Syntax Description

number	Total number of transmissions per transaction. The default is eight.

Defaults

Eight transmissions

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Use this command to specify the maximum number of transmissions that may be retried per transaction on a RADIUS server. This command has no meaning if the **radius-server retry method order** command has not been already configured.

Examples

The following example shows that a RADIUS server has been configured for six retries per transaction:

```
aaa new-model
radius-server retry method reorder
radius-server retransmit 0
radius-server transaction max-tries 6
radius-server host 192.2.3.4
radius-server host 192.6.7.8
```

Related Commands

Command	Description
radius-server retry method reorder	Specifies the reordering of RADIUS traffic retries among a server group.

radius-server unique-ident

To enable the acct-session-id-count variable containing the unique identifier variable, use the **radius-server unique-ident** command in global configuration mode. To disable the acct-session-id-count variable, use the **no** form of this command.

radius-server unique-ident *id*

no radius-server unique-ident

Syntax Description

id	Unique identifier represented by the first eight bits of the acct-session-id-count variable. Valid values range from 0 to 255.

Defaults

The acct-session-id-count variable is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.

Usage Guidelines

Use the **radius-server unique-ident** command to increase the size of the accounting session identifier (ID) variable from 32 bits to 56 bits.

RADIUS attribute 44, Accounting Session ID, is a unique accounting identifier that makes it easy to match start and stop records in a log file. Accounting session ID numbers restart at 1 each time the router is power-cycled or the software is reloaded.

The acct-session-id variable is a 32-bit variable that can take on values from 00000000–FFFFFFFF.

The acct-session-id-count variable enabled by the **radius-server unique-ident** command is a 32-bit variable. The first eight bits of the variable are reserved for the unique identifier, an identifier that allows the RADIUS server to identify an accounting session if a reload occurs. The remaining 24 bits of the acct-session-id-count variable acts as a counter variable. When the first acct-session-id variable is assigned, the acct-session-id-count variable is set to 1. The acct-session-id-count variable increments by one every time the acct-session-id variable wraps.

The acct-session-id-count variable can take on values from ##000000–##FFFFFF, where ## represents the eight bits that are reserved for the unique identifier variable.

The acct-session-id-count and acct-session-id variables are concatenated before being sent to the RADIUS server, resulting in the accounting session being represented by the following 56-bit variable:

##000000 00000000–##FFFFFF FFFFFFFF

Examples

The following example shows how to enable the acct-session-id-count variable and sets the unique identifier variable to 5:

```
radius-server unique-ident 5
```

radius-server vsa disallow unknown

To configure the IOS to deny access when the RADIUS server returns unknown Vendor-Specific Attributes (VSAs) in its Access-Accept attribute, use the **radius-server vsa disallow unknown** command in global configuration mode.

To permit access when the RADIUS server sends unknown VSAs, use the **no** form of this command.

radius-server vsa disallow unknown

no radius-server vsa disallow unknown

Command Default

Not enabled

Command Modes

Global configuration: Router(config)#

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

It is suggested that unknown VSAs should be ignored by RADIUS clients. If an Access-Accept attribute is received that includes an attribute of unknown type, then a RADIUS client can assume that it is a potential service definition, and treat it as an Access-Reject attribute. However, there may be interoperability issues with the above suggestion, and this is why the **no** form of this command may be used in certain scenarios to configure the IOS to permit access when the RADIUS server sends unknown VSAs.

Related Commands

Command	Description
radius-server vsa send	Configures the network access server (NAS) to recognize and use VSAs.

radius-server vsa send

To configure the network access server (NAS) to recognize and use vendor-specific attributes (VSAs), use the **radius-server vsa send** command in global configuration mode. To restore the default, use the **no** form of this command.

radius-server vsa send [**accounting** | **authentication** | **cisco-nas-port**] [**3gpp2**]

no radius-server vsa send [**accounting** | **authentication** | **cisco-nas-port**] [**3gpp2**]

Syntax Description

accounting	(Optional) Limits the set of recognized VSAs to only accounting attributes.
authentication	(Optional) Limits the set of recognized VSAs to only authentication attributes.
cisco-nas-port	(Optional) Due to the Internet Engineering Task Force (IETF) requirement for including NAS port information in attribute 87 (Attr87), the Cisco NAS port is obsoleted by default. However, if your servers require this information, then the **cisco-nas-port** keyword can be used to return the Cisco NAS port VSA.
3gpp2	(Optional) Adds Third Generation Partnership Project 2 (3gpp2) Cisco VSAs to this packet type.

Command Default

NAS is not configured to recognize and use VSAs.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3T	This command was introduced.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. The **cisco-nas-port** and **3gpp2** keywords were added to provide backward compatibility for Cisco VSAs.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.3S.	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

The IETF draft standard specifies a method for communicating vendor-specific information between the NAS and the RADIUS server by using the VSA (attribute 26). VSAs allow vendors to support their own extended attributes not suitable for general use. The **radius-server vsa send** command enables the NAS to recognize and use both accounting and authentication VSAs. Use the **accounting** keyword with the **radius-server vsa send** command to limit the set of recognized VSAs to accounting attributes only. Use the **authentication** keyword with the **radius-server vsa send** command to limit the set of recognized VSAs to authentication attributes only.

The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. The Cisco vendor ID is 9, and the supported option has vendor-type 1, which is named "cisco-avpair." The value is a string with the following format:

```
protocol : attribute sep value *
```

In the preceding example, "protocol" is a value of the Cisco "protocol" attribute for a particular type of authorization; "attribute" and "value" are an appropriate attribute-value (AV) pair defined in the Cisco TACACS+ specification; and "sep" is "=" for mandatory attributes and "*" for optional attributes. This solution allows the full set of features available for TACACS+ authorization to also be used for RADIUS.

For example, the following AV pair causes the Cisco "multiple named ip address pools" feature to be activated during IP authorization (during the PPP Internet Protocol Control Protocol (IPCP) address assignment):

```
cisco-avpair= "ip:addr-pool=first"
```

The following example causes a "NAS Prompt" user to have immediate access to EXEC commands.

```
cisco-avpair= "shell:priv-lvl=15"
```

Other vendors have their own unique vendor IDs, options, and associated VSAs. For more information about vendor IDs and VSAs, see RFC 2138, *Remote Authentication Dial-In User Service (RADIUS)*.

Examples

The following example shows how to configure the NAS to recognize and use vendor-specific accounting attributes:

```
Router(config)# radius-server vsa send accounting
```

Related Commands

Command	Description
aaa nas port extended	Replaces the NAS-Port attribute with RADIUS IETF attribute 26 and displays extended field information.

rate-limit (firewall)

To limit the number of Layer 7 Session Initiation Protocol (SIP) or H.323 protocol messages that strike the Cisco IOS firewall every second, use the **rate-limit** command in policy-map-class configuration mode. To remove the rate limit from the configuration, use the **no** form of this command.

rate-limit *limit-number*

no rate-limit *limit-number*

Syntax Description

limit-number	Number of application messages allowed per second. Range: 1 to 2147483647.

Command Default

No rate limit is configured.

Command Modes

Policy-map-class configuration (config-pmap-c)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	Support for the H.323 protocol was introduced.

Usage Guidelines

Use this command when configuring a rate-limiting mechanism to monitor the call attempt rate and the number of calls per second for the H.323 or SIP protocol.

The **rate-limit** command is used with the **policy-map type inspect** command and must be configured with the **class type inspect** command.

When configuring a rate-limiting mechanism for the H.323 or SIP protocol, the **rate-limit** command is used with the appropriate **match** command to choose the required control messages. For the H.323 protocol, the **rate limit** command is used with the **match message** command. For the SIP protocol, the **rate limit** command is used with the **match request** command.

Examples

The following example configures a rate limiting mechanism of 5 invite messages per second for the SIP class map “my_sip_rt_msgs”:

```
class-map type inspect sip match-any my_sip_rt_msgs
 match request method invite
 policy-map type inspect sip my_sip_policy
 class type inspect sip my_sip_rt_msgs
 rate-limit 5
```

The following example configures a rate-limiting mechanism of 16 setup messages per second to monitor the call attempt rate for H.323 protocol based calls:

```
class-map type inspect h323 match-any my_h323_rt_msgs
 match message setup
 policy-map type inspect h323 my_h323_policy
 class type inspect h323 my_h323_rt_msgs
 rate-limit 16
```

Related Commands

Command	Description
class type inspect	Specifies the class on which an action is to be performed.
match message	Configures the match criterion for a class map on the basis of H.323 protocol messages.
policy-map type inspect	Creates an inspect type policy map.

rd

To specify a route distinguisher (RD) for a VPN routing and forwarding (VRF) instance, use the **rd** command in VRF configuration mode. To remove a route distinguisher, use the **no** form of this command.

rd *route-distinguisher*

no rd *route-distinguisher*

Syntax Description

route-distinguisher	An 8-byte value to be added to an IPv4 prefix to create a VPN IPv4 prefix.

Command Default

No RD is specified.

Command Modes

VRF configuration (config-vrf)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	Support for IPv6 was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(54)SG	This command was integrated into Cisco IOS Release 12.2(54)SG.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

An RD creates routing and forwarding tables and specifies the default route distinguisher for a VPN. The RD is added to the beginning of the customer's IPv4 prefixes to change them into globally unique VPN-IPv4 prefixes.

An RD is either:

- ASN-related—Composed of an autonomous system number and an arbitrary number.
- IP-address-related—Composed of an IP address and an arbitrary number.

You can enter an RD in either of these formats:

16-bit autonomous-system-number:*your 32-bit number*
For example, 101:3.

32-bit IP address:*your 16-bit number*
For example, 192.168.122.15:1.

Examples

The following example shows how to configure a default RD for two VRFs. It illustrates the use of both autonomous-system-number-relative and IP-address-relative RDs:

```
Router(config)# ip vrf vrf1
Router(config-vrf)# rd 100:3
Router(config-vrf)# exit
Router(config)# ip vrf vrf2
Router(config-vrf)# rd 10.13.0.12:200
```

The following is an example of a VRF for IPv4 and IPv6 that has common policies defined in the global part of the VRF configuration:

```
vrf definition vrf2
 rd 200:1
 route-target both 200:2
!
 address-family ipv4
 exit-address-family
!
 address-family ipv6
 exit-address-family
 end
```

Related Commands

Command	Description
ip vrf	Configures a VRF routing table.
show ip vrf	Displays the set of defined VRFs and associated interfaces.
vrf definition	Configures a VRF routing table and enters VRF configuration mode.

reauthentication time

To enter the time limit after which the authenticator should reauthenticate, use the **reauthentication time** command in local RADIUS server group configuration mode. To remove the requirement that users reauthenticate after the specified duration, use the **no** form of this command.

reauthentication time *seconds*

no reauthentication time *seconds*

Syntax Description

seconds	Number of seconds after which reauthentication occurs. Range is from 1 to 4294967295. Default is 0.

Defaults

0 seconds, which means group members are not required to reauthenticate.

Command Modes

Local RADIUS server group configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Examples

The following example shows that the time limit after which the authenticator should reauthenticate is 30 seconds:

```
Router(config-radsrv-group)# reauthentication time 30
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.

Command	Description
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

redirect (identity policy)

To redirect clients to a particular URL, use the **redirect** command in identity policy configuration mode. To remove the URL, use the **no** form of this command.

redirect url *url*

no redirect url *url*

Syntax Description

url	URL to which clients should be redirected.
url	Valid URL.

Defaults

No default behavior or values

Command Modes

Identity policy configuration (config-identity-policy)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

When you use this command, an identity policy has to be associated with an Extensible Authentication Protocol over UDP (EAPoUDP) identity profile.

Examples

The following example shows the URL to which clients are redirected:

```
Router (config)# identity policy p1
Router (config-identity-policy)# redirect url http://www.example.com
```

Related Commands

Command	Description
identity policy	Creates an identity policy.

redundancy (GDOI)

To enable Group Domain of Interpretation (GDOI) redundancy configuration mode and to allow for key server redundancy, use the **redundancy** command in GDOI local server configuration mode. To disable GDOI redundancy, use the **no** form of this command.

redundancy

no redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

Key server redundancy is not supported for a key server.

Command Modes

GDOI local server configuration (config-local-server)

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

This command must be configured before configuring related redundancy commands, such as for key server peers, local priority, and timer values. Use the **local priority** command to set the local key server priority. Use the **peer address ipv4** command to configure the peer address that belongs to the redundancy key server group.

Examples

The following example shows that key server redundancy has been configured:

```
address ipv4 10.1.1.1
redundancy
 local priority 10
 peer address ipv4 10.41.2.5
 peer address ipv4 10.33.5.6
```

Related Commands

Command	Description
address ipv4	Sets the source address, which is used as the source for packets originated by the local key server.
local priority	Sets the local key server priority.
peer address ipv4	Configures the peer key server.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

redundancy group

To configure the virtual IP address for the redundancy group, use the **redundancy group** command in interface configuration mode**.** To remove virtual IP address from the redundancy group, use the **no** form of this command.

redundancy group *id* **ip** *address* **exclusive** [**decrement** *value*]

no redundancy group *id* **ip** *address* **exclusive** [**decrement** *value*]

Syntax Description

id	Redundancy group ID.
ip *address*	Specifies the IP address of the interface.
exclusive	Specifies whether the interface is not shared with another redundancy group.
decrement *value*	(Optional) Amount decremented from the priority when the L1 state of the interface goes down. This overrides the default amount for the redundancy group. The range is from 1 to 255.

Command Default

Virtual IP address is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The virtual IP address and the physical address must in the same subnet.

Examples

The following example shows how to configure the virtual IP address for the redundancy group:

```
Router# configure terminal
Router(config)# interface GigabitEthernet0/1/1
Router(config-if)# redundancy group 2 ip 10.2.3.4 exclusive
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
control	Configures the control interface type and number for a redundancy group.
data	Configures the data interface type and number for a redundancy group.

Command	Description
group	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.
protocol	Defines a protocol instance in a redundancy group.
redundancy rii	Configures the RII for the redundancy group.

redundancy inter-device

To enter inter-device configuration mode, use the **redundancy inter-device** command in global configuration mode. To exit inter-device configuration mode, use the **exit** command. To remove all inter-device configuration, use the no form of this command.

redundancy inter-device

no redundancy inter-device

Syntax Description

This command has no arguments or keywords.

Defaults

If this command is not enabled, you cannot configure stateful failover for IPSec.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the **redundancy inter-device** command to enter inter-device configuration mode, which allows you to enable and protect Stateful Switchover (SSO) traffic.

Examples

The following example shows how to issue the **redundancy inter-device** command when enabling SSO:

```
redundancy inter-device
 scheme standby HA-in
!
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.0.0.1
   remote-port 5000
    remote-ip 10.0.0.2
!
```

The following example shows how to issue the **redundancy inter-device** command when configuring SSO traffic protection:

```
crypto ipsec transform-set trans2 ah-md5-hmac esp-aes
!
crypto ipsec profile sso-secure
 set transform-set trans2
!
redundancy inter-device
 scheme standby HA-in
 security ipsec sso-secure
```

Related Commands

Command	Description
local-ip	Defines at least one local IP address that is used to communicate with the redundant peer.
local-port	Defines the local SCTP that is used to communicate with the redundant peer.
remote-ip	Defines at least one IP address of the redundant peer that is used to communicate with the local device.
remote-port	Defines the remote SCTP that is used to communicate with the redundant peer.
scheme	Defines that redundancy scheme that is used between two devices.

redundancy rii

To configure the redundancy interface identifier (RII) for the redundancy group protected traffic interfaces, use the **redundancy rii** command in interface configuration mode**.** To remove the control interface from the redundancy group, use the **no** form of this command.

redundancy rii *id*

no redundancy rii *id*

SyntaxDescription

id	Redundancy interface identifier. The range is from 1 to 65535.

Command Default

RII is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

Every interface associated with one or more redundancy groups must have a unique RII assigned to it. RII allows interfaces to have a one-to-one mapping between peers.

Examples

The following example shows how to configure the RII for the Gigabit Ethernet interface:

```
Router# configure terminal
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# redundancy rii 100
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
control	Configures the control interface type and number for a redundancy group.
data	Configures the data interface type and number for a redundancy group.
group	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.

Command	Description
protocol	Defines a protocol instance in a redundancy group.
redundancy group	Configures the virtual IP address for a redundancy group.

redundancy stateful

To configure stateful failover for tunnels using IP Security (IPSec), use the **redundancy stateful** command in crypto map configuration mode. To disable stateful failover for tunnel protection, use the **no** form of this command.

redundancy *standby-group-name* **stateful**

no redundancy *standby-group-name* **stateful**

Syntax Description

standby-group-name	Refers to the name of the standby group as defined by Hot Standby Router Protocol (HSRP) standby commands. Both routers in the standby group are defined by this argument and share the same virtual IP (VIP) address.

Defaults

Stateful failover is not enabled for IPSec tunnels.

Command Modes

Crypto map configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

The **redundancy stateful** command uses an existing IPSec profile (which is specified via the **crypto ipsec profile** command) to configure IPSec stateful failover for tunnel protection. (You do not configure the tunnel interface as you would with a crypto map configuration.) IPSec stateful failover enables you to define a backup IPSec peer (secondary) to take over the tasks of the active (primary) router if the active router is deemed unavailable.

The tunnel source address must be a VIP address, and it must not be an interface name.

Examples

The following example shows how to configure stateful failover for tunnel protection:

```
crypto ipsec profile peer-profile
  redundancy HA-out stateful

interface Tunnel1
 ip unnumbered Loopback0
 tunnel source 209.165.201.3
 tunnel destination 10.0.0.5
 tunnel protection ipsec profile peer-profile
!
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 name HA-out
```

Related Commands

Command	Description
crypto ipsec profile	Defines the IPSec parameters that are to be used for IPSec encryption between two routers and enters crypto map configuration mode.

regenerate

To enable key rollover with manual certificate enrollment, use the **regenerate** command in ca-trustpoint configuration mode. To disable key rollover, use the **no** form of this command.

regenerate

no regenerate

Syntax Description

This command has no arguments or keywords.

Defaults

Key rollover is not enabled.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **regenerate** command to provide seamless key rollover for manual certificate enrollment. A new key pair is created with a temporary name, and the old certificate and key pair are retained until a new certificate is received from the certification authority (CA). When the new certificate is received, the old certificate and key pair are discarded and the new key pair is renamed with the name of the original key pair.

If the key pair being rolled over is exportable, the new key pair will also be exportable. The following comment will appear in the trustpoint configuration to indicate whether the key pair is exportable:

```
! RSA keypair associated with trustpoint is exportable
```

Do not regenerate the keys manually; key rollover will occur when the **crypto ca enroll** command is issued.

Examples

The following example shows how to configure key rollover to regenerate new keys with a manual certificate enrollment from the CA named “trustme2”.

```
crypto ca trustpoint trustme2
 enrollment url http://trustme2.company.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet0
 serial-number none
```

```
 regenerate
 password revokeme
 rsakeypair trustme2 2048
 exit
crypto ca authenticate trustme2
crypto ca enroll trustme2
```

Related Commands

Command	Description
crypto ca authenticate	Retrieves the CA certificate and authenticates it.
crypto ca enroll	Requests certificates from the CA for all of your router's RSA key pairs.
crypto ca trustpoint	Declares the CA that your router should use.

regexp (profile map configuration)

To create an entry in a cache profile group that allows authentication and authorization matches based on a regular expression, use the **regexp** command in profile map configuration mode. To disable a regular expression entry, use the **no** form of this command.

regexp *matchexpression* {**any** | **only**} [**no-auth**]

no regexp *matchexpression* {**any** | **only**}

Syntax Description

matchexpression	String representing a regular expression on which to match.
any	Specifies that any unique instance of a AAA server response that matches the regular expression is saved in the cache.
only	Specifies that only one instance of a AAA server response that matches the regular expression is saved in the cache.
no-auth	(Optional) Specifies that authentication is bypassed for this user.

Command Default

No regular expression entries are defined.

Command Modes

Profile map configuration (config-profile-map)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use this command to create an entry in a cache profile group that matches based on a regular expression, such as .*@example.com or .*@xyz.com.

Because the number of entries in a regular expression cache profile group could be in the thousands, and validating each request against a regular expression can be time consuming, we do not recommend using regular expression entries in cache profile groups.

Examples

The following example creates an entry in the cache profile group networkusers that authorizes network access to any example company user. No authentication is performed for these users because the **no-auth** keyword is used.

```
Router# configure terminal
Router(config)# aaa cache profile networkusers
Router(config-profile-map)# regexp .*@example.com any no-auth
```

Related Commands

Command	Description
profile	Creates an individual authentication and authorization cache profile based on an exact username match.

registration interface

To specify the interface to be used for a Group Domain of Interpretation (GDOI) registration, use the **registration interface** command in GDOI local server configuration mode. To disable an interface, use the **no** form of this command.

registration interface *type slot/port*

no registration interface *type slot/port*

Syntax Description

type	Type of interface (see Table 60 below).
slot/port	Slot and port number of the interface.

Command Default

None

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Table 60 lists the types of interface that may be used for the *type* argument.

Table 60 Type of Interface

Interface	Description
Async	Async interface
BVI	Bridge-Group Virtual Interface
CDMA-1x	Code division multiple access 1x interface
CTunnel	CTunnel interface
Dialer	Dialer interface
Ethernet	Institute of Electrical and Electronics Engineers (IEEE) Standard 802.3
Lex	Lex interface
Loopback	Loopback interface
MFR	Multilink Frame Relay bundle interface
Multilink	Multilink group interface
Null	Null interface
Serial	Serial
Tunnel	Tunnel interface

Table 60 Type of Interface (continued)

Interface	Description
Vif	Pragmatic General Multicast (PGM) Multicast Host interface
Virtual-PPP	Virtual PPP interface
Virtual-Template	Virtual Template interface
Virtual-TokenRing	Virtual TokenRing

Examples

The following example shows that the interface is Ethernet 0/0:

```
registration interface Ethernet 0/0
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration.

rekey address ipv4

To specify the source or destination information of the rekey message, use the **rekey address ipv4** command in GDOI local server configuration mode. To remove a source or destination address, use the **no** form of this command.

rekey address ipv4 {*access-list-number* | *access-list-name*}

no rekey address ipv4 {*access-list-number* | *access-list-name*}

Syntax Description

access-list-number	IP access list number. The number can be from 100 through 199, or it can be in the expanded range of 2000 through 2699.
access-list-name	Access list name.

Command Default

None

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

If rekeys are not required, this command is optional. If rekeys are required, this command is required.

The source is usually the key server interface from which the message leaves, and the destination is the multicast address on which the group members receive the rekeys (for example, access-list 101 permit 121 permit udp host 10.0.5.2 eq 848 host 192.168.1.2. eq 848).

Examples

The following example shows that the rekey address is access list "101":

```
rekey address ipv4 101
```

The following example shows that a rekey message is to be sent to access control list (ACL) address 239.10.10.10:

```
crypto gdoi group gdoigroup1
 identity number 1111
 server local
  rekey address ipv4 120
  rekey lifetime seconds 400
  no rekey retransmit
  rekey authentication mypubkey rsa ipseca-3845b.examplecompany.com
access-list 120 permit udp host 10.5.90.1 eq 848 host 239.10.10.10 eq 848
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration.

rekey algorithm

To define the type of encryption algorithm used for a Group Domain of Interpretation (GDOI) group, use the **rekey algorithm** command in GDOI local server configuration mode. To disable an algorithm that was defined, use the **no** form of this command.

rekey algorithm {*type-of-encryption-algorithm*}

no rekey algorithm {*type-of-encryption-algorithm*}

Syntax Description

type-of-encryption-algorithm	Type of encryption algorithm used (see Table 61). The default algorithm is 3des-cbc. • The rekey algorithm is used to encrypt the rekey message that is sent from the key server to the multicast group.

Command Default

If this command is not configured, the default value of 3des-cbc takes effect. However, the default is used only if the commands required for a rekey to occur are specified (see the Note below in "Usage Guidelines").

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Table 61 lists the types of encryption algorithms that may be used.

Table 61 Types of Encryption

Encryption Type	Description
3des-cbc	Cipher Block Chaining mode of the Triple Data Encryption Standard (3des).
aes 128	128-bit Advanced Encrytion Standard (AES).
aes 192	192-bit AES.
aes 256	256-bit AES.
des-cbc	Cipher Block Chaining mode of the Data Encryption Standard (des).

Note At a minimum, the following commands are required for a rekey to occur:

rekey address ipv4 {*access-list-number* | *access-list-name*}

rekey authentication {**mypubkey** | **pubkey**} {*rsa key-name*}

If the **rekey algorithm** command is not configured, the default of 3des-cbc is used if the above minimum rekey configuration is met.

Examples

The following example shows that the 3des-cbc encryption standard is used:

```
rekey algorithm 3des-cbc
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
rekey address ipv4	Specifies the source or destination information of the rekey message.
rekey authentication	Specifies the keys to be used to a rekey to GDOI group members.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

rekey authentication

To specify the keys to be used for a rekey to Group Domain of Interpretation (GDOI) group members, use the **rekey authentication** command in GDOI local server configuration mode. To disable the keys, use the **no** form of this command.

rekey authentication {**mypubkey** | **pubkey**} {**rsa** *key-name*}

no rekey authentication {**mypubkey** | **pubkey**} {**rsa** *key-name*}

Syntax Description

mypubkey	Keypair associated with this device.
pubkey	Public key associated with a different device.
rsa	Identifies an Rivest, Shamir, and Adelman (RSA) keypair.
key-name	Key to be used for rekey.

Command Default

None

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

If rekeys are not required, this command is optional. If rekeys are required, this command is required.

For this command to work, Rivest, Shamir, and Adelman (RSA) keys must be generated first on the router using the following command:

crypto key generate rsa {**general keys**} [**label** *key-label*]

For example:

```
crypto key generate rsa general keys label group_1234_key_name
```

Examples

The following example shows that the keypair to be used for a rekey is RSA “group_1234_key_name”:

```
rekey authentication mypubkey rsa group_1234_key_name
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
crypto key generate rsa	Generates RSA key pairs.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration.

rekey lifetime

To limit the number of seconds for which any one encryption key should be used, use the **rekey lifetime** command in GDOI local server configuration mode. To disable the number of seconds that were set, use the **no** form of this command.

rekey lifetime {**seconds** *number-of-seconds*}

no rekey lifetime {**seconds** *number-of-seconds*}

Syntax Description

number-of-seconds	Lifetime in seconds. Value: 300 through 86400 seconds.

Command Default

If this command is not configured, the default value of 86400 seconds takes effect.

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This **rekey** command is not used often. When this rekey limit is sent, a new key encryption key is sent to the group member so that the next rekey after this one will be encrypted with the new key encryption key.

Examples

The following example shows that the rekey lifetime has been set to 600 seconds:

```
rekey lifetime seconds 600
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

rekey retransmit

To specify the number of times the rekey message is retransmitted, use the **rekey retransmit** command in GDOI local server configuration mode. To disable the number of times that were specified, use the **no** form of this command.

rekey retransmit {*number-of-seconds*} [**number** *number-of-retransmissions*]

no rekey retransmit {*number-of-seconds*} [**number** *number-of-retransmissions*]

Syntax Description

number-of-seconds	Number of seconds that the rekey message is retransmitted. Range: 10 through 60. Default=10.
number *number-of-retransmissions*	Number of times the message may be retransmitted. Range: 1 through 10. Default: 2.

Command Default

If this command is not configured, the number of seconds defaults to 10 and the number of transmissions defaults to 2.

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Use this command if you are concerned about network loss. Using this command ensures that the rekey message is resent the number of times specified in the retransmit command.

Examples

The following example shows that the rekey message may be retransmitted twice for 15 seconds each time:

```
rekey retransmit 15 number 2
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

rekey transport unicast

To configure unicast delivery of rekey messages to group members, use the **rekey transport unicast** command in global configuration mode. To remove unicast delivery of rekey messages and enable the default to multicast rekeying, use the **no** form of this command.

rekey transport unicast

no rekey transport unicast

Syntax Description

This command has no arguments or keywords.

Command Default

If **rekey transport unicast** is not specified or **no rekey transport unicast** is specified, multicast rekeying is the default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

This command is configured on the key server under the **server local** command, along with other rekey configurations.

Examples

The following example shows that unicast delivery of rekey messages to group members has been configured:

```
crypto gdoi group diffint
 identity number 3333
 server local
  rekey lifetime seconds 300
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa mykeys
  rekey transport unicast
  sa ipsec 1
   profile gdoi-p
   match address ipv4 120
   replay counter window-size 64
   address ipv4 10.0.5.2
```

Related Commands

Command	Description
address ipv4	Sets the source address, which is used as the source for packets originated by the local key server.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

remark

To write a helpful comment (remark) for an entry in a named IP access list, use the **remark** command in access list configuration mode. To remove the remark, use the **no** form of this command.

remark *remark*

no remark *remark*

Syntax Description

remark	Comment that describes the access-list entry, up to 100 characters long.

Defaults

The access-list entries have no remarks.

Command Modes

Standard named or extended named access list configuration

Command History

Release	Modification
12.0(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The remark can be up to 100 characters long; anything longer is truncated.

If you want to write a comment about an entry in a numbered IP access list, use the **access-list remark** command.

Examples

In the following example, the host1 subnet is not allowed to use outbound Telnet:

```
ip access-list extended telnetting
 remark Do not allow host1 subnet to telnet out
 deny tcp host 172.69.2.88 any eq telnet
```

Related Commands

Command	Description
access-list remark	Specifies a helpful comment (remark) for an entry in a numbered IP access list.
deny (IP)	Sets conditions under which a packet does not pass a named IP access list.
ip access-list	Defines an IP access list by name.
permit (IP)	Sets conditions under which a packet passes a named IP access list.

replay counter window-size

To turn on counter-based anti-replay protection for traffic defined inside an access list using Group Domain of Interpretation (GDOI) if there are only two group members in a group, use the **replay counter window-size** command in GDOI SA IPsec configuration mode. To disable counter-based anti-replay protection, use the **no** form of this command.

replay counter window-size [*number*]

no replay counter window-size

Syntax Description

number	Size of the Sychronous Anti-Replay (SAR) clock window expressed in bytes. Values are equal to 64, 128, 256, 512, and 1024 bytes. Default window size is 64 bytes.

Command Default

Counter-based anti-replay is not enabled.

Command Modes

GDOI SA IPsec configuration (gdoi-sa-ipsec)

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

This command is configured on the key server.

Cisco IPsec authentication provides anti-replay protection against an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet. (Security association [SA] anti-replay is a security service in which the receiver can reject old or duplicate packets to protect itself against replay attacks.) The decryptor checks off the sequence numbers that it has seen before. The encryptor assigns sequence numbers in an increasing order. The decryptor remembers the value X of the highest sequence number that it has already seen. N is the window size in bytes, and the decryptor also remembers whether it has seen packets having sequence numbers from X-N+1 through X. Any packet with the sequence number X-N is discarded. Currently, N is set at 64, so only 64 packets can be tracked by the decryptor.

At times, however, the 64-packet window size is not sufficient. For example, Cisco quality of service (QoS) gives priority to high-priority packets, which could cause some low-priority packets to be discarded even though they could be one of the last 64 packets received by the decryptor. The IPsec Anti-Replay Window: Expanding and Disabling feature allows you to expand the window size, allowing the decryptor to keep track of more than 64 packets.

Increasing the anti-replay window size has no impact on throughput and security. The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed to store the sequence number on the decryptor. It is recommended that you use the full 1024 window size to eliminate any future anti-replay problems.

Note GDOI anti-replay can be either counter based or time based. Use this command for counter-based anti-replay protection. For time-based anti-replay protection, use the **replay time window-size** command.

Examples

The following example shows that the anti-replay window size for unicast traffic has been set to 512:

```
crypto gdoi group gdoigroup1
 identity number 1111
 server local
  rekey address ipv4 120
  rekey lifetime seconds 400
  no rekey retransmit
  rekey authentication mypubkey rsa ipseca-3845b.examplecompany.com
 sa ipsec 10
   profile group1111
   match address ipv4 101
   replay counter window-size 512
```

Related Commands

Command	Description
replay time window-size	Sets the the window size for anti-replay protection using GDOI if there are more than two group members in a group.
sa ipsec	Specifies the IPsec SA policy information to be used for a GDOI group and enters GDOI SA IPsec configuration mode.

replay time window-size

To set the window size for anti-replay protection using Group Domain of Interpretation (GDOI) if there are more than two group members in a group, use the **replay time window-size** command in GDOI SA IPsec configuration mode. To disable time-based anti-replay, use the **no** form of this command.

replay time window-size *seconds*

no replay time window-size

Syntax Description

seconds	Number of seconds of the interval duration of the Sychronous Anti-Replay (SAR) clock. The value range is 1 through 100. The default value is 100.

Command Default

Time-based anti-replay is not enabled.

Command Modes

GDOI SA IPsec configuration (gdoi-sa-ipsec)

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

This command is configured on the key server.

Note GDOI anti-replay can be either counter based or time based. This command turns on time-based anti-replay. For counter-based anti-replay protection, use the **replay counter window-size** command.

Examples

The following example shows that the number of seconds of the interval duration of the SAR clock has been set to 1:

```
sa ipsec 10
 profile group1111
 match address ipv4 101
 replay time window-size 1
```

Related Commands

Command	Description
replay counter window-size	Sets the window size for counter-based anti-replay protection for unicast traffic defined inside an access list.
sa ipsec	Specifies the IPsec SA policy information to be used for a GDOI group and enters GDOI SA IPsec configuration mode.

request-method

To permit or deny HTTP traffic according to either the request methods or the extension methods, use the **request-method** command in appfw-policy-http configuration mode. To disable this inspection parameter, use the **no** form of this command.

request-method {**rfc** *rfc-method* | **extension** *extension-method*} **action** {**reset** | **allow**} [**alarm**]

no request-method {**rfc** *rfc-method* | **extension** *extension-method*} **action** {**reset** | **allow**} [**alarm**]

Syntax Description

rfc	Specifies that the supported methods of RFC 2616, *Hypertext Transfer Protocol—HTTP/1.1*, are to be used for traffic inspection.
rfc-method	Any one of the following RFC 2616 methods can be specified: **connect**, **default, delete**, **get**, **head**, **options**, **post**, **put**, **trace**.
extension	Specifies that the extension methods are to be used for traffic inspection.
extension-method	Any one of the following extension methods can be specified: **copy**, **default, edit**, **getattribute**, **getproperties**, **index**, **lock**, **mkdir**, **move**, **revadd**, **revlabel**, **revlog**, **save**, **setattribute**, **startrev**, **stoprev**, **unedit, unlock**.
action	Methods and extension methods outside of the specified method are subject to the specified action (**reset** or **allow**).
reset	Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection.
allow	Forwards the packet through the firewall.
alarm	(Optional) Generates system logging (syslog) messages for the given action.

Defaults

If a given method is not specified, all methods and extension methods are supported with the reset alarm action.

Command Modes

appfw-policy-http configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Only methods configured by the **request-method** command are allowed thorough the firewall; all other HTTP traffic is subjected to the specified action (**reset** or **allow**).

Examples

The following example shows how to define the HTTP application firewall policy “mypolicy.” This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule “firewall,” which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

request-timeout

To set the number of seconds before an authentication request times out, use the **request-timeout** command in webvpn sso server configuration mode.

request-timeout *number-of-seconds*

no request-timeout *number-of-seconds*

Syntax Description

number-of-seconds	Number of seconds. Value = 10 through 30. Default = 15.

Command Default

None

Command Modes

Webvpn sso server configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

This command is useful for networks that are congested and tend to have losses. Corporate networks are generally not affected by congestion or losses.

Examples

The following example shows that the number of seconds before an authentication request times out is 25:

```
webvpn context context1
 sso-server test-sso-server
  request-timeout 25
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

reset (policy-map)

To reset an SMTP connection with an SMTP sender (client) if it violates the specified policy, use the **reset** command in policy-map configuration mode. This action sends an error code to the sender and closes the connection gracefully.

reset

Command Default No default behavior or values.

Command Modes Policy-map configuration

Command History

12.4(20)T	This command was introduced in Cisco IOS Release 12.4(20)T.

Examples The following example displays the reset command configuration for DSP 1:

```
Router(config)# policy-map type inspect smtp p1
Router(config-pmap)# class type inspect smtp c1
Router(config-pmap)# reset
```

reset (zone-based policy)

To reset a TCP connection if the data length of the Simple Mail Transfer Protocol (SMTP) body exceeds the value that you configured in the **class-map type inspect smtp** command, use the **reset** command in policy-map configuration mode.

reset

Syntax Description

This command has no arguments or keywords.

Command Default

The TCP connection is not reset.

Command Modes

Policy-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use this command only after entering the **policy-map type inspect**, **class type inspect**, and **parameter-map type inspect** commands.

You can enter **reset** only for TCP traffic.

Examples

The following example creates a Layer 7 SMTP policy map named mysmtp-policy and applies the reset action to each of the match criteria:

```
policy-map type inspect smtp mysmtp-policy
 class-map type inspect smtp huge-mails
  reset
```

Related Commands

Command	Description
class type inspect	Specifies the traffic (class) on which an action is to be performed.
parameter-map type inspect	Configures an inspect type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
policy-map type inspect	Creates Layer 3 and Layer 4 inspect type policy maps.

responder-only

To configure a device as responder-only, use the **responder-only** command in IPsec profile configuration mode. To remove the responder-only setting, use the no form of this command.

responder-only

no responder-only

Syntax Description

This command has no arguments or keywords.

Command Default

A device is not configured as responder-only.

Command Modes

IPsec profile configuration (ipsec-profile)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

This command is relevant only for a virtual interface scenario and is configurable only under an IPsec profile. Neither static nor crypto maps are supported.

Examples

The following example shows that the device has been configured as a responder-only:

```
crypto ipsec profile vti
 set transform-set 3dessha
 set isakmp-profile clients
 responder-only
```

Related Commands

Command	Description
crypto ipsec profile	Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec routers and enters IPsec profile configuration mode.

retired (IPS)

specify whether or not a retired signature or signature category definition should be saved in the router memory, use the **retired** command in signature-definition-status (config-sigdef-status) or IPS-category-action (config-ips-category-action) configuration mode. To return to the default action, use the **no** form of this command.

retired {**true** | **false**}

no retired

Syntax Description

true	Retires all signatures within a given category.
false	"Unretires" all signatures within a given category.

Command Default

Signature or signature category definitions are not saved in the system.

Command Modes

Signature-definition-status configuration (config-sigdef-status)
IPS-category-action configuration (config-ips-category-action)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Router memory and resource constraints prevent a router from loading all Cisco IOS IPS signatures. Thus, it is recommended that you load only a selected set of signatures that are defined by the categories. Because the categories are applied in a "top-down" order, you should first retire all signatures, followed by "unretiring" specific categories. Retiring signatures enables the router to load information for all signatures, but the router will not build the parallel scanning data structure.

Retired signatures are not scanned by Cisco IOS IPS, so they will not fire alarms. If a signature is irrelevant to your network or if you want to save router memory, you should retire signatures, as appropriate.

Examples

The following example shows how to retire all signatures and configure the Basic "ios_ips" category:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ips signature category
Router(config-ips-category)# category all
Router(config-ips-category-action)# retired true
Router(config-ips-category-action)# exit
Router(config-ips-category)# category ios_ips basic
Router(config-ips-category-action)# retired false
Router(config-ips-category-action)# exit
Router(config-ips-category)# exit
Do you want to accept these changes? [confirm]y
```

Related Commands

Command	Description
enabled	Changes the enabled status of a given signature or signature category.
signature	Specifies a signature for which the CLI user tunings will be changed.
status	Enters the signature-definition-status configuration mode, which allows you to change the enabled or retired status of an individual signature.

reverse-route

To create source proxy information for a crypto map entry, use the **reverse-route** command in crypto map configuration mode. To remove the source proxy information from a crypto map entry, use the **no** form of this command.

Effective with Cisco IOS Release 12.4(15)T

reverse-route [**static** | **remote-peer** *ip-address* [**gateway**] [**static**]]

no reverse-route [**static** | **remote-peer** *ip-address* [**gateway**] [**static**]]

Before Cisco IOS Release 12.4(15)T

reverse-route [**static** | **tag** *tag-id* [**static**] | **remote-peer** [**static**] | **remote-peer** *ip-address* [**static**]]

no reverse-route [static | tag *tag-id* **[static] | remote-peer [static] | remote-peer** *ip-address* [**static**]]

Syntax Description

tag *tag-id*	(Optional) Tag value that can be used as a "match" value for controlling redistribution via route maps. **Note** The **tag** keyword and *tag-id* argument were deleted effective with Cisco IOS Release 12.4(15)T.
remote-peer	(Optional) Indicates two routes: one for the tunnel endpoint, with the next hop being the interface to which the crypto map is bound. **Note** The **remote-peer** keyword and its variants (*ip-address* argument and **gateway** keyword) are applicable only to crypto maps.
ip-address	(Optional) If used without the optional **gateway** keyword, there is only one route: the protected subnet. The next hop is determined by the user-added value for the *ip-address* argument.
gateway	(Optional) Used with the *ip-address* argument. If the **gateway** keyword is used, there are two routes: one to the protected subnet by way of the remote-tunnel endpoint and the other to the remote-tunnel endpoint that is determined by the user-added value for the *ip-address* argument. **Note** The optional **gateway** keyword enables the behavior of the **reverse-route remote-peer** *ip-address* command syntax used for software releases before Cisco IOS Release 12.3(14)T.
static	(Optional) Creates routes on the basis of crypto ACLs, regardless of whether flows have been created for these ACLs.

Defaults

No default behavior or values.

Command Modes

Crypto map configuration (config-crypto-map)

Command History

Release	Modification
12.1(9)E	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5800 platforms.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S.
12.2(13)T	The **remote-peer** keyword and *ip-address* argument were added.
12.3(14)T	The **static** and **tag** keywords and *tag-id* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)T	The **tag** keyword and *tag-id* argument were deleted. The **gateway** keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command can be applied on a per-crypto map basis.

Reverse route injection (RRI) provides a scalable mechanism to dynamically learn and advertise the IP address and subnets that belong to a remote site that connects through an IP Security (IPSec) Virtual Private Network (VPN) tunnel.

When enabled in an IPSec crypto map, RRI will learn all the subnets from any network that is defined in the crypto ACL as the destination network. The learned routes are installed into the local routing table as static routes that point to the encrypted interface. When the IPSec tunnel is torn down, the associated static routes will be removed. These static routes may then be redistributed into other dynamic routing protocols so that they can be advertised to other parts of the network (usually done by redistributing RRI routes into dynamic routing protocols on the core side).

Examples

Before Cisco IOS Release 12.3(14)T

The following is an example in which RRI has been configured when crypto ACLs exist. The example shows that all remote VPN gateways connect to the router via 192.168.0.3. RRI is added on the static crypto map, which creates routes on the basis of the source network and source netmask that are defined in the crypto ACL.

```
crypto map mymap 1 ipsec-isakmp
 set peer 10.1.1.1
 reverse-route
 set transform-set esp-3des-sha
 match address 102

Interface FastEthernet 0/0
 ip address 192.168.0.2 255.255.255.0
 standby name group1
 standby ip 192.168.0.3
 crypto map mymap redundancy group1

access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
```

Note In Cisco IOS Release 12.3(14)T and later releases, for the static map to retain this same behavior of creating routes on the basis of crypto ACL content, the **static** keyword will be necessary, that is, **reverse-route static.**

The **reverse-route** command in this situation creates routes that are analogous to the following static route command-line interface (CLI) commands (**ip route**):

- Remote Tunnel Endpoint

  ```
  ip route 10.1.1.1 255.255.255.255 192.168.1.1
  ```

- VPN Services Module (VPNSM)

  ```
  ip route 10.1.1.1 255.255.255.255 vlan0.1
  ```

In the following example, two routes are created, one for the remote endpoint and one for route recursion to the remote endpoint via the interface on which the crypto map is configured.

```
reverse-route remote-peer
```

Configuring RRI with the Enhancements Added in Cisco IOS Release 12.3(14)T

The following configuration example shows that RRI has been configured for a situation in which there are existing ACLs:

```
crypto map mymap 1 ipsec-isakmp
   set peer 172.17.11.1
   reverse-route static
   set transform-set esp-3des-sha
   match address 101

access-list 101 permit ip 192.168.1.0 0.0.0.255 172.17.11.0 0.0.0.255
```

The following example shows how RRI-created routes can be tagged with a tag number and then used by a routing process to redistribute those tagged routes via a route map:

```
crypto dynamic-map ospf-clients 1
 reverse-route tag 5

router ospf 109
 redistribute rip route-map rip-to-ospf

route-map rip-to-ospf permit
 match tag 5
 set metric 5
 set metric-type type1

Router# show ip ospf topology

P 10.81.7.48/29, 1 successors, FD is 2588160, tag is 5
  via 192.168.82.25 (2588160/2585600), FastEthernet0/1
```

The following example shows that one route has been created to the remote proxy via a user-defined next hop. This next hop should not require a recursive route lookup unless it will recurse to a default route.

```
reverse-route remote-peer 10.4.4.4
```

The previous example yields the following before Cisco IOS Release 12.3(14)T:

```
10.0.0.0/24 via 10.1.1.1 (in the VRF table if VRFs are configured)
10.1.1.1/32 via 10.4.4.4 (in the global route table)
```

And this result occurs with RRI enhancements:

```
10.0.0.0/24 via 10.4.4.4 (in the VRF table if VRFs are configured, otherwise in the global
table)
```

Effective with Cisco IOS Release 12.4(15)T

In the following example, routes are created from the destination information in the access control list (ACL). One route will list 10.2.2.2 as the next hop route to the ACL information, and one will indicate that to get to 10.2.2.2, the route will have to go by way of 10.1.1.1. All routes will have a metric of 10. Routes are created only at the time the map and specific ACL rule are created.

```
crypto map map1 1 ipsec-isakmp
 set peer 10.2.2.2
 reverse-route remote-peer 10.1.1.1 gateway
 set reverse-route distance 10
 match address 101
Configuring RRI with Route Tags 12.4(15)T or later: Example
```

The following example shows how RRI-created routes can be tagged with a tag number and then used by a routing process to redistribute those tagged routes via a route map:

```
crypto dynamic-map ospf-clients 1
 set reverse-route tag 5

router ospf 109
 redistribute rip route-map rip-to-ospf

route-map rip-to-ospf permit
 match tag 5
 set metric 5
 set metric-type type1

Router# show ip ospf topology

P 10.81.7.48/29, 1 successors, FD is 2588160, tag is 5
  via 192.168.82.25 (2588160/2585600), FastEthernet0/1
```

Related Commands

Command	Description
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
show crypto map (IPSec)	Displays the crypto map configuration.

revocation-check

To check the revocation status of a certificate, use the **revocation-check** command in ca-trustpoint configuration mode. To disable this functionality, use the **no** form of this command.

revocation-check *method1* [*method2*[*method3*]]

no revocation-check *method1* [*method2*[*method3*]]

Syntax Description

method1 [*method2*[*method3*]]	Method used by the router to check the revocation status of the certificate. Available methods are as follows: • **crl**—Certificate checking is performed by a certificate revocation list (CRL). This is the default behavior. • **none**—Certificate checking is not required. • **ocsp**—Certificate checking is performed by an online certificate status protocol (OCSP) server. If a second and third method are specified, each method will be used only if the previous method returns an error, such as a server being down.

Defaults

After a trustpoint is enabled, the default is set to **revocation-check crl**, which means that CRL checking is mandatory.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(2)T	This command was introduced. This command replaced the **crl best-effort** and **crl optional** commands.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

Use the **revocation-check** command to specify at least one method that is to be used to ensure that the certificate of a peer has not been revoked.

If your router does not have the applicable CRL and is unable to obtain one or if the OCSP server returns an error, your router will reject the peer's certificate—unless you include the **none** keyword in your configuration. If the **none** keyword is configured, a revocation check will not be performed and the certificate will always be accepted. If the **revocation-check none** command is configured, you cannot manually download the CRL via the **crypto pki crl request** command because the manually downloaded CRL may not be deleted after it expires. The expired CRL can cause all certificate verifications to be denied.

Note The **none** keyword replaces the **optional** keyword that is available from the **crl** command. If you enter the **crl optional** command, it will be written back as the **revocation-check none** command. However, there is a difference between the **crl optional** command and the **revocation-check none** command. The **crl optional** command will perform revocation checks against any applicable in-memory CRL. If a CRL is not available, a CRL will not be downloaded and the certificate is treated as valid; the **revocation-check none** command ignores the revocation check completely and always treats the certificate as valid.

Also, the **crl** and **none** keywords issued together replace the **best-effort** keyword that is available from the **crl** command. If you enter the **crl best-effort** command, it will be written back as the **revocation-check crl none** command.

Examples

The following example shows how to configure the router to use the OCSP server that is specified in the AIA extension of the certificate:

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# revocation-check ocsp
```

The following example shows how to configure the router to download the CRL from the CDP; if the CRL is unavailable, the OCSP server that is specified in the Authority Info Access (AIA) extension of the certificate will be used. If both options fail, certificate verification will also fail.

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# revocation-check crl ocsp
```

The following example shows how to configure your router to use the OCSP server at the HTTP URL "http://myocspserver:81." If the server is down, revocation check will be ignored.

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# ocsp url http://myocspserver:81
Router(ca-trustpoint)# revocation-check ocsp none
```

Related Commands

Command	Description
crl query	Queries the CRL to ensure that the certificate of the peer has not been revoked.
crypto pki trustpoint	Declares the CA that your router should use.
ocsp url	Enables an OCSP server.

root

To obtain the certification authority (CA) certificate via TFTP, use the **root** command in ca-trustpoint configuration mode. To deconfigure the CA, use the **no** form of this command.

root tftp *server-hostname filename*

no root tftp *server-hostname filename*

Syntax Description

tftp	Defines the TFTP protocol to get the root certificate.
server-hostname filename	Specifies a name for the server and a name for the file that will store the trustpoint CA.

Defaults

A CA certificate is not configured.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command allows you to access the CA via the TFTP protocol, which is used to get the CA. You want to configure a CA certificate so that your router can verify certificates issued to peers. Thus, your router does not have to enroll with the CA that issued the certificates the peers.

Before you can configure this command, you must enable the **crypto ca trustpoint** command, which puts you in ca-trustpoint configuration mode.

Note The **crypto ca trustpoint** command deprecates the **crypto ca identity** and **crypto ca trusted-root** commands and all related subcommands (all ca-identity and trusted-root configuration mode commands). If you enter a ca-identity or trusted-root subcommand, the configuration mode and command will be written back as ca-trustpoint.

Examples

The following example shows how to configure the CA certificate named “bar” using TFTP:

```
crypto ca trustpoint bar
 root tftp xxx fff
 crl optional
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

root CEP

The **crypto ca trustpoint** command deprecates the **crypto ca trusted-root** command and all related subcommands (all trusted-root configuration mode commands). If you enter a trusted-root subcommand, the configuration mode and command will be written back as ca-trustpoint.

root PROXY

The **root PROXY** command is replaced by the **enrollment http-proxy** command. See the **enrollment http-proxy** command for more information.

root TFTP

The **root TFTP** command is replaced by the **root** command. See the **root** command for more information.

rsakeypair

To specify which Rivest, Shamir, and Adelman (RSA) key pair to associate with the certificate, use the **rsakeypair** command in ca-trustpoint configuration mode.

rsakeypair *key-label* [*key-size* [*encryption-key-size*]]

Syntax Description

key-label	Name of the key pair, which is generated during enrollment if it does not already exist or if the **auto-enroll regenerate** command is configured.
key-size	(Optional) Size of the desired Rivest, Shamir, Adelman (RSA) key pair. If the size is not specified, the existing key size is used.
encryption-key-size	(Optional) Size of the second key, which is used to request separate encryption, signature keys, and certificates.

Defaults

The fully qualified domain name (FQDN) key is used.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) command was added.

Usage Guidelines

When you regenerate a key pair, you are responsible for reenrolling the identities associated with the key pair. Use the **rsakeypair** command to refer back to the named key pair.

Examples

The following example is a sample trustpoint configuration that specifies the RSA key pair "exampleCAkeys":

```
crypto ca trustpoint exampleCAkeys
 enroll url http://exampleCAkeys/certsrv/mscep/mscep.dll
 rsakeypair exampleCAkeys 1024 1024
```

Related Commands

Command	Description
auto-enroll	Enables autoenrollment.
crl	Generates RSA key pairs.
crypto ca trustpoint	Declares the CA that your router should use.

rsa-pubkey

To define the Rivest, Shamir, and Adelman (RSA) manual key to be used for encryption or signature during Internet Key Exchange (IKE) authentication, use the **rsa-pubkey** command in keyring configuration mode. To remove the manual key that was defined, use the **no** form of this command.

rsa-pubkey{**address** *address* | **name** *fqdn*} [**encryption** | **signature**]

no rsa-pubkey {**address** *address* | **name** *fqdn*} [**encryption** | **signature**]

Syntax Description

address *address*	IP address of the remote peer.
name *fqdn*	Fully qualified domain name (FQDN) of the peer.
encryption	(Optional) The manual key is to be used for encryption.
signature	(Optional) The manual key is to be used for signature.

Defaults

No default behavior or values

Command Modes

Keyring configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Use this command to enter public key chain configuration mode. Use this command when you need to manually specify RSA public keys of other IP Security (IPSec) peers. You need to specify the keys of other peers when you configure RSA encrypted nonces as the authentication method in an IKE policy at your peer router.

Examples

The following example shows that the RSA public key of an IPSec peer has been specified:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```

sa ipsec

To specify the IP security (IPsec) security association (SA) policy information to be used for a Group Domain of Interpretation (GDOI) group and to enter GDOI SA IPsec configuration mode, use the **sa ipsec** command in GDOI local server configuration mode. To remove the policy information that was specified, use the **no** form of this command.

sa ipsec {*sequence-number*}

no sa ipsec {*sequence-number*}

Syntax Description

sequence-number	Sequence number of the IPsec SA.

Command Default

None

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

IPsec and SA policy information must be specified using this command if the traffic encryption key policy has to be defined.

Examples

The following example shows that three IPsec SA policy numbers (1, 2, and 3) have been specified:

```
sa ipsec 1
  profile gdoi-p
  match address ipv4 120
sa ipsec 2
  profile gdoi-q
  match address ipv4 121
sa ipsec 3
  profile gdoi-r
  match address ipv4 122
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
match address	Specifies an IP extended access list for a GDOI registration.
profile	Defines the IPsec SA policy for a GDOI group.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

sa receive-only

To specify that an IP security (IPsec) security association (SA) is to be installed by a group member as "inbound only," use the **sa receive-only** command in GDOI local server configuration mode. To remove the inbound-only specification, use the **no** form of this command.

sa receive-only

no sa receive-only

Syntax Description

This command has no arguments or keywords.

Command Default

If this command is not configured, IPsec SAs are installed by group members as both inbound and outbound.

Command Modes

GDOI local server configuration (config-local-server)

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

This command is configured on a key server. The command may be used to ease in deployment.

Examples

The following example shows that the Group Domain of Interpretation (GDOI) group is instructed by the key server to install the IPsec SAs as "inbound only":

```
crypto gdoi group gdoi_group
 identity number 1234
server local
 sa receive-only
 sa ipsec 1
  profile gdoi-p
  match address ipv4 120
```

Related Commands

Command	Description
crypto gdoi gm	Allows group members to change the IPsec SA status.
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

save-password

To save your extended authentication (Xauth) password locally on your PC, use the **save-password** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To disable the Save-Password attribute, use the **no** form of this command.

save-password

no save-password

Syntax Description

This command has no arguments or keywords.

Defaults

Your Xauth password is not saved locally on your PC, and the Save-Password attribute is not added to the server group profile.

Command Modes

ISAKMP group configuration (config-isakmp-group)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

Save password control allows you to save your Xauth password locally on your PC so that after you have initially entered the password, the Save-Password attribute is pushed from the server to the client. On subsequent authentications, you can activate the password by using the tick box on the software client or by adding the username and password to the Cisco IOS hardware client profile. The password setting remains until the Save-Password attribute is removed from the server group profile. After the password has been activated, the username and password are sent automatically to the server during Xauth without your intervention.

The save-password option is useful only if your password is static, that is, if it is not a one-time password such as one that is generated by a token.

The Save-Password attribute is configured on a Cisco IOS router or in the RADIUS profile.

To configure save password control, use the **save-password** command.

An example of an attribute-value (AV) pair for the Save-Password attribute is as follows:

```
ipsec:save-password=1
```

You must enable the **crypto isakmp client configuration group** command, which specifies group policy information that has to be defined or changed, before enabling the **save-password** command.

Note

- The Save-Password attribute can be applied only by a RADIUS user.

- The attribute can be applied on a per-user basis after the user has been authenticated.
- The attribute can override any similar group attributes.
- User-based attributes are available only if RADIUS is used as the database.

Examples

The following example shows that the Save-Password attribute has been configured:

```
crypto isakmp client configuration group cisco
 save-password
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto isakmp client configuration group	Specifies the DNS domain to which a group belongs.

scheme

To define the redundancy scheme that is used between two devices, use the **scheme** command in inter-device configuration mode. To disable the redundancy scheme, use the **no** form of this command.

scheme standby *standby-group-name*

no scheme standby *standby-group-name*

Syntax Description

standby	Redundancy scheme. Currently, the standby scheme is the only available scheme.
standby-group-name	Specifies the name of the standby group. This name must match the name that was specified via the **standby name** command. Also, the standby name should be the same on both the active and standby routers.

Defaults

A redundancy scheme is not specified.

Command Modes

Inter-device configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Only the active or standby state of the standby group is used for Stateful Switchover (SSO). The virtual IP (VIP) address of the standby group is not required or used by SSO. Also, the standby group does not have to be part of any crypto map configuration.

Examples

The following example shows how to enable SSO and define the standby scheme that is to be used by the active and standby devices:

```
redundancy inter-device
 scheme standby HA-in
!
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.0.0.1
   remote-port 5000
    remote-ip 10.0.0.2
```

Related Commands

Command	Description
standby name	Configures the name of the standby group.

search-filter

To configure a search request sent by the Lightweight Directory Access Protocol (LDAP) client to the server in order to find the user's node in the Directory Information Tree (DIT), use the **search-filter** command in LDAP server configuration mode. To delete the search request from the LDAP server group, use the **no** form of this command.

search-filter user-object-type *string*

no search-filter user-object-type *string*

Syntax Description

user-object-type	Adds a user attribute to the search filter.
string	Name of the object class attribute.

Command Default

No default search requests are configured.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

You can add multiple search filter attributes by using the **search-filter** command. The search filter is a mandatory configuration for an LDAP server, because it is used to filter the exact user from the search results. Without this configuration, a user cannot be authenticated. The **search-filter** command helps you to filter the search results based on the attributes mentioned in the search filter.

Examples

The following example shows how to filter the search results for an LDAP server. After you have specified the search criteria as shown below, the search filter string appears in the "(&(objectclass=person) (&(cn=$userid)(cid=$contextid)))" format.

```
Router(config)# ldap server server1
Router(config-ldap-server)# search-filter user-object-type cn
Router(config-ldap-server)# search-filter user-object-type cid
Router(config-ldap-server)# search-filter user-object-type objectclass
```

Related Commands

Command	Description
ldap server	Defines an LDAP server and enters LDAP server configuration mode.

secondary-color

To configure the color of the secondary title bars on the login and portal pages of a SSL VPN website, use the **secondary-color** command in webvpn context configuration mode. To remove the color from the WebVPN context configuration, use the **no** form of this command.

secondary-color *color*

no secondary-color *color*

Syntax Description

color	The value for the *color* argument is entered as a comma-separated red, green, blue (RGB) value, an HTML color value (beginning with a"#"), or the name of the color that is recognized in HTML (no spaces between words or characters). The value is limited to 32 characters. The value is parsed to ensure that it matches one of the following formats (using Perl regex notation): • \#/x{6} • \d{1,3},\d{1,3},\d{1,3} (and each number is from 1 to 255) • \w+ The default color is purple.

Defaults

The color purple is used if this command is not configured or if the **no** form is entered.

Command Modes

Webvpn context configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Configuring a new color overrides the color of the preexisting color.

Examples

The following examples show the three forms in which the secondary color is configured:

```
Router(config-webvpn-context)# secondary-color darkseagreen
Router(config-webvpn-context)# secondary-color #8FBC8F
Router(config-webvpn-context)# secondary-color 143,188,143
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

secondary-text-color

To configure the color of the text on the secondary bars of an SSL VPN website, use the **secondary-text-color** command in webvpn context configuration mode. To revert to the default color, use the **no** form of this command.

secondary-text-color [**black** | **white**]

no secondary-text-color [**black** | **white**]

Syntax Description

black	(Optional) Color of the text is black. This is the default value.
white	(Optional) Color of the text is white.

Defaults

The color of the text on secondary bars is black if this command is not configured or if the **no** form is entered.

Command Modes

Webvpn context configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The color of the text on the secondary bars must be aligned with the color of the text on the title bar.

Examples

The following example sets the secondary text color to white:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# secondary-text-color white
Router(config-webvpn-context)#
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

secret

To associate a command-line interface (CLI) view or a superview with a password, use the **secret** command in view configuration mode.

secret {[**0**] *unencrypted-password* | **5** *encrypted-password*}

Syntax Description

unencrypted-password	Nonencrypted password. A password can contain any combination of alphanumeric characters. The password is case sensitive. This clear-text password will be encrypted using the message digest 5 (MD5) method.
0	Specifes that an unencrypted password will follow.
5	Specifes that an encrypted password will follow.
encrypted-password	Encrypted password that you enter and that is copied from another router configuration.

Defaults

The user cannot access a CLI view or superview.

Command Modes

View configuration (config-view)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

A user cannot access any commands within the CLI view or superview until the **secret** command has been issued.

Note The password cannot be removed, but you can overwrite it.

Examples

The following examples show how to configure two CLI views, “first” and “second,” and associate each view with a password:

CLI View “first”

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# parser view first
Router(config-view)#
*Dec  9 05:20:03.039: %PARSER-6-VIEW_CREATED: view 'first' successfully created.
Router(config-view)# secret firstpassword
Router(config-view)# secret secondpassword
```

```
% Overwriting existing secret for the current view
Router(config-view)# secret 0 thirdpassword
% Overwriting existing secret for the current view
Router(config-view)# secret 5 $1$jj1e$vmYyRbmj5UoU96tT1x7eP1
% Overwriting existing secret for the current view
Router(config-view)# secret 5 invalidpassword
ERROR: The secret you entered is not a valid encrypted secret.
To enter an UNENCRYPTED secret, do not specify type 5 encryption.
When you properly enter an UNENCRYPTED secret, it will be encrypted.

Router(config-view)# command exec include show version
Router(config-view)# command exec include configure terminal
Router(config-view)# command configure include all ip
Router(config-view)# exit
```

CLI View "second"

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# parser view second
Router(config-view)#
*Dec 30 06:11:52.915: %PARSER-6-VIEW_CREATED: view 'second' successfully created.
Router(config-view)# secret mypasswd
Router(config-view)# commands exec include ping
Router(config-view)# end

Router# show running-config

parser view second
 secret 5 $1$PWs8$lz3lSx6OqAnFrUx2hkI0w0
 commands exec include ping
!
```

The following is an example of **show running-config** output for a situation in which the **secret** command has been configured using a level 5 encrypted password:

```
Router: show running-config

parser view first
 secret 5 $1$jj1e$vmYyRbmj5UoU96tT1x7eP1
 commands configure include all ip
 commands exec include configure terminal
 commands exec include configure
 commands exec include show version
 commands exec include show
!
```

Related Commands

Command	Description
parser view	Creates or changes a CLI view and enters view configuration mode.

secret-key

To configure the policy server secret key that is used to secure authentication requests, use the **secret-key** command in webvpn sso server configuration mode. To remove the secret key, use the **no** form of this command.

secret-key *key-name*

no secret-key *key-name*

Syntax Description

key-name	Name of secret key.

Command Default

A policy server secret key is not configured.

Command Modes

Webvpn sso server configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Note

- A web agent URL and policy server secret key are required for a Single SignOn (SSO) server configuration. If the web agent URL and policy server secret key are not configured, a warning message is displayed. (See the Warning Message section in the Examples section below.)
- This is the same secret key that should be configured on the Cisco SiteMinder plug-in.

Examples

The following example shows the policy server secret key is “example.123”:

```
webvpn context context1
 sso-server test-sso-server
  secret-key example.123
```

Warning Message

If a web agent URL and policy server secret key are not configured, a message similar to the following is received:

```
Warning: must configure web agent URL for sso-server “example”
Warning: must configure SSO policy server secret key for sso-server “example”
Warning: invalid configuration. SSO for “example” being disabled
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

secure boot-config

To take a snapshot of the router running configuration and securely archive it in persistent storage, use the **secure boot-config** command in global configuration mode. To remove the secure configuration archive and disable configuration resilience, use the **no** form of this command.

secure boot-config [**restore** *filename*]

no secure boot-config

Syntax Description

restore *filename*	(Optional) Reproduces a copy of the secure configuration archive as the supplied filename.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Without any parameters, this command takes a snapshot of the router running configuration and securely archives it in persistent storage. Like the image, the configuration archive is hidden and cannot be viewed or removed directly from the command-line interface (CLI) prompt . It is recommended that you run this command after the router has been fully configured to reach a steady state of operation and the running configuration is considered complete for a restoration, if required. A syslog message is printed on the console notifying the user of configuration resilience activation. The secure archive uses the time of creation as its filename. For example, .runcfg-20020616-081702.ar was created July 16 2002 at 8:17:02.

The restore option reproduces a copy of the secure configuration archive as the supplied filename (disk0:running-config, slot1:runcfg, and so on). The restore operation will work only if configuration resilience is enabled. The number of restored copies that can be created is unlimited.

The **no** form of this command removes the secure configuration archive and disables configuration resilience. An enable, disable, enable sequence has the effect of upgrading the configuration archive if any changes were made to the running configuration since the last time the feature was disabled.

The configuration upgrade scenario is similar to an image upgrade. The feature detects a different version of Cisco IOS and notifies the user of a version mismatch. The same command can be run to upgrade the configuration archive to a newer version after new configuration commands corresponding to features in the new image have been issued.

The correct sequence of steps to upgrade the configuration archive after an image upgrade is as follows:

- Configure new commands
- Issue the **secure boot-config** command

Examples

The following example shows the command used to securely archive a snapshot of the router running configuration:

```
secure boot-config
```

The following example shows the command used to restore an archived image to the file slot0:rescue-cfg:

```
Router(config)# secure boot-config restore slot0:rescue-cfg
ios resilience:configuration successfully restored as slot0:rescue-cfg
```

Related Commands

Command	Description
secure boot-image	Enables Cisco IOS image resilience.
show secure bootset	Displays the status of image and configuration resilience.

secure boot-image

To enable Cisco IOS image resilience, use the **secure boot-image** command in global configuration mode. To disable Cisco IOS image resilience and release the secured image so that it can be safely removed, use the **no** form of this command.

secure boot-image

no secure boot-image

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

This command enables or disables the securing of the running Cisco IOS image. The following two possible scenarios exist with this command.

- When turned on for the first time, the running image (as displayed in the **show version** command output) is secured, and a syslog entry is generated. This command will function properly only when the system is configured to run an image from a disk with an Advanced Technology Attachment (ATA) interface. Images booted from a TFTP server cannot be secured. Because this command has the effect of "hiding" the running image, the image file will not be included in any directory listing of the disk. The **no** form of this command releases the image so that it can be safely removed.
- If the router is configured to boot up with Cisco IOS resilience and an image with a different version of Cisco IOS is detected, a message similar to the following is displayed at bootup:

```
ios resilience :Archived image and configuration version 12.2 differs from running
version 12.3.
Run secure boot-config and image commands to upgrade archives to running version.
```

To upgrade the image archive to the new running image, reenter this command from the console. A message will be displayed about the upgraded image. The old image is released and will be visible in the **dir** command output.

Caution Be careful when copying new images to persistent storage because the existing secure image name might conflict with the new image. To verify the name of the secured archive, run the **show secure bootset** command and resolve any name conflicts with the currently secured hidden image.

Note After the Cisco IOS image is secured, the resilient configuration feature will deny any requests to copy, modify, or delete the secure archive and will even survive a disk format operation.

Examples

The following example shows the activation of image resilience.

```
Router(config)# secure boot-image
```

Related Commands

Command	Description
dir	Displays a list of files on a file system.
secure boot-config	Saves a secure copy of the router running configuration in persistent storage.
show secure bootset	Displays the status of image and configuration resilience.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

secure cipher

To specify the ciphersuite in case of secure connection, use the **secure cipher** command in Lightweight Directory Access Protocol (LDAP) server configuration mode. To disable the secure connection, use the **no** form of this command.

secure cipher {**3des-ede-cbc-sha** | **des-cbc-sha** | **rc4-128-md5** | **rc4-128-sha** | **null-md5**} [**3des-ede-cbc-sha**] [**des-cbc-sha**] [**rc4-128-md5**] [**rc4-128-sha**] [**null-md5**]

no secure cipher {**3des-ede-cbc-sha** | **des-cbc-sha** | **rc4-128-md5** | **rc4-128-sha**} [**3des-ede-cbc-sha**] [**des-cbc-sha**] [**rc4-128-md5**] [**rc4-128-sha**] [**null-md5**]

SyntaxDescription

3des-ede-cbc-sha	Specifies the encryption null MD5 ciphersuite.
des-cbc-sha	Specifies encryption ssl_rsa_with_rc4_128_md5 ciphersuite.
rc4-128-md5	Specifies encryption ssl_rsa_with_rc4_128_md5 ciphersuite.
rc4-128-sha	Specifies encryption ssl_rsa_with_rc4_128_sha ciphersuite.
null-md5	Encryption null MD5 ciphersuite.

Command Default

If no ciphersuite is specified, all ciphersuites are considered.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

A ciphersuite is a set of authentication, encryption, and data integrity algorithms used for exchanging messages between network nodes. During a Secure Socket Layer (SSL) handshake, for example, the two nodes negotiate to see which cipher uite they will use when transmitting messages back and forth.

The **secure cipher** command specifies the crypto methods supported by the Lightweight Directory Access Protocol (LDAP) client in Cisco IOS software. This command is applicable only when the **mode secure** command is enabled.

Examples

The following example shows how to configure the crypto methods that are supported by LDAP in Cisco IOS software:

```
Router(config)# ldap server server1
Router(config-ldap-server)# secure cipher des-cbc-sha
```

Related Commands

Command	Description
ldap server	Defines an LDAP server and enters LDAP server configuration mode.
mode secure	Enables the security mode in LDAP server.

security (Diameter peer)

To configure the security protocol for the Diameter peer connection, use the **security** command in Diameter peer configuration mode. To disable the configured protocol, use the **no** form of this command.

security {**ipsec** | **tls**}

no security {**ipsec** | **tls**}

Syntax Description

ipsec	IP security protocol.
tls	Transport layer security.

Command Default

IP security (IPsec) is the default security protocol for Diameter peer connections.

Command Modes

Diameter peer configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

If you dynamically change the security protocol for a Diameter peer, the connection to that peer is broken. When you exit the Diameter peer configuration submode, the connection is reestablished.

Examples

The following example shows how to configure IPsec for a Diameter peer:

```
Router (config-dia-peer)# security ipsec
```

Related Commands

Command	Description
diameter peer	Configures a Diameter peer and enters Diameter peer configuration submode.
show diameter peer	Displays the Diameter peer configuration.

security authentication failure rate

To configure the number of allowable unsuccessful login attempts, use the **security authentication failure rate** command in global configuration mode. To disable this functionality, use the **no** form of this command.

security authentication failure rate *threshold-rate* **log**

no security authentication failure rate *threshold-rate* **log**

Syntax Description

threshold-rate	Number of allowable unsuccessful login attempts. The valid value range for the *threshold-rate* argument is 2 to 1024. The default is 10.
log	Syslog authentication failures if the rate exceeds the threshold.

Defaults

The default number of failed login attempts before a 15-second delay is 10.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.3(7)T	The range of the *threshold-rate* value was changed from 1 through 1024 to 2 through 1024.

Usage Guidelines

The **security authentication failure rate** command provides enhanced security access to the router by generating syslog messages after the number of unsuccessful login attempts exceeds the configured threshold rate. This command ensures that there are not any continuous failures to access the router.

Note Previous to the Cisco IOS software release 12.3(7)T the *threshold-rate* value range was 1 through 1024. Unsuccessful login attempts will not be logged if a value of 1 is configured. As of Cisco ISO release 12.3(7)T, use a value between 2 and 1024.

Examples

The following example shows how to configure your router to generate a syslog message after eight failed login attempts:

```
security authentication failure rate 8 log
```

Related Commands

Command	Description
security passwords min-length	Ensures that all configured passwords are at least a specified length.

security ipsec

To apply a previously configured IP Security (IPSec) profile to the redundancy group communications, use the **security ipsec** command in inter-device configuration mode. To remove the IPSec profile from the configuration, use the **no** form of this command.

security ipsec *profile-name*

no security [**ipsec** [*profile-name*]]

Syntax Description

profile-name	Profile name, which was specified via the **crypto ipsec profile** command.

Defaults

The redundancy group is not secured.

Command Modes

Inter-device configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

The **security ipsec** command allows you to secure a redundancy group via a previously configured IPSec profile. If you are certain that the Stateful Switchover (SSO) traffic between the redundancy group runs on a physically secure interface, you do not have to configure this command.

Note If you configure SSO traffic protection via the **security ipsec** command, the active and standby devices must be directly connected to each other via Ethernet networks.

Examples

The following example shows how to configure SSO traffic protection:

```
crypto ipsec transform-set trans2 ah-md5-hmac esp-aes
!
crypto ipsec profile sso-secure
 set transform-set trans2
!
redundancy inter-device
 scheme standby HA-in
 security ipsec sso-secure
```

Related Commands

Command	Description
crypto ipsec profile	Defines the IPSec parameters that are to be used for IPSec encryption between two IPSec routers.
redundancy inter-device	Enters inter-device configuration mode.

security passwords min-length

To ensure that all configured passwords are at least a specified length, use the **security passwords min-length** command in global configuration mode. To disable this functionality, use the **no** form of this command.

security passwords min-length *length*

no security passwords min-length *length*

Syntax Description

length	Minimum length of a configured password. The default is six characters.

Defaults

Six characters

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

The **security passwords min-length** command provides enhanced security access to the router by allowing you to specify a minimum password length, eliminating common passwords that are prevalent on most networks, such as “lab” and “cisco.” This command affects user passwords, enable passwords and secrets, and line passwords. After this command is enabled, any password that is less than the specified length will fail.

Examples

The following example shows both how to specify a minimum password length of six characters and what happens when the password does not adhere to the minimum length:

```
security password min-length 6
enable password lab
% Password too short - must be at least 6 characters. Password not configured.
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
security authentication failure rate	Configures the number of allowable unsuccessful login attempts.

self-identity

To define the identity that the local Internet Key Exchange (IKE) uses to identify itself to the remote peer, use the **self-identity** command in ISAKMP profile configuration mode. To remove the Internet Security Association and Key Management Protocol (ISAKMP) identity that was defined for the IKE, use the **no** form of this command.

self-identity {**address** | **address ipv6**] | **fqdn** | **user-fqdn** *user-fqdn*}

no self-identity {**address** | **address ipv6**] | **fqdn** | **user-fqdn** *user-fqdn*}

Syntax Description

address	The IP address of the local endpoint.
address ipv6	The IPv6 address of the local endpoint.
fqdn	The fully qualified domain name (FQDN) of the host.
user-fqdn *user-fqdn*	The user FQDN that is sent to the remote endpoint.

Command Default

If no ISAKMP identity is defined in the ISAKMP profile configuration, global configuration is the default.

Command Modes

ISAKMP profile configuration (config-isa-prof)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(4)T	The **address ipv6** keyword was added.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Examples

The following example shows that the IKE identity is the user FQDN “user@vpn.com”:

```
crypto isakmp profile vpnprofile
 self-identity user-fqdn user@vpn.com
```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile and audits IPSec user sessions.

serial-number (ca-trustpoint)

To specify whether the router serial number should be included in the certificate request, use the **serial-number** command in ca-trustpoint configuration mode. To restore the default behavior, use the **no** form of this command.

serial-number [**none**]

no serial-number

Syntax Description

none	(Optional) Specifies that a serial number will not be included in the certificate request.

Defaults

Not configured. You will be prompted for the serial number during certificate enrollment.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) command was introduced.

Usage Guidelines

Before you can issue the **serial-number** command, you must enable the **crypto ca trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.

Use this command to specify the router serial number in the certificate request, or use the **none** keyword to specify that a serial number should not be included in the certificate request.

Examples

The following example shows how to omit a serial number from the "root" certificate request:

```
crypto ca trustpoint root
 enrollment url http://10.3.0.7:80
 ip-address none
 fqdn none
 serial-number none
 subject-name CN=jack, OU=PKI, O=Cisco Systems, C=US

crypto ca trustpoint root
 enrollment url http://10.3.0.7:80
 serial-number
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

serial-number (pubkey)

To define the serial number for the Rivest, Shamir, and Adelman (RSA) manual key to be used for encryption or signatures during Internet Key Exchange (IKE) authentication, use the **serial-number** command in pubkey configuration mode. To remove the manual key that was defined, use the **no** form of this command.

serial-number *serial-number*

no serial-number *serial-number*

Syntax Description

serial-number	Device serial number. The value is from 0 through infinity.

Defaults

No default behavior or values

Command Modes

Pubkey configuration (config-pubkey-key)

Command History

Release	Modification
12.2(15)T	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Examples

The following example shows that the public key of an IP Security (IPSec) peer has been specified:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey-key)# serial-number 1000000
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```

Related Commands

Command	Description
address	Specifies the IP address of the remote RSA public key of the remote peer that you will manually configure.
key-string (IKE)	Specifies the RSA public key of a remote peer.

server (application firewall policy)

To configure a set of Domain Name System (DNS) servers for which the specified instant messenger application will be interacting, use the **server** command in the appropriate configuration mode. To change or remove a configured set of DNS servers, use the **no** form of this command.

server {**permit** | **deny**} {**name** *string* | **ip-address** {*ip-address* | **range** *ip-address-start ip-address-end*}

no server {**permit** | **deny**} {**name** *string* | **ip-address** {*ip-address* | **range** *ip-address-start ip-address-end*}

Syntax Description

permit	Inspects all traffic destined for a specified server, and the applicable policy is enforced.
deny	Blocks all traffic destined for a specified, denied server. TCP connections are denied by dropping all packets bound to the specified server.
name *string*	Name of DNS server for which traffic will be permitted (and inspected) or denied. The same server name cannot appear under two different instant messenger applications; however, the same name can appear under two different policies within the same instant messenger application. Each entry will accept only one DNS name.
ip-address	Indicates that at least one IP address will be listed.
ip-address	IP address of the DNS server for which traffic will be permitted (and inspected) or denied.
range *ip-address-start ip-address-end*	Range of DNS server IP addresses for which traffic will be permitted (and inspected) or denied.

Command Default

If this command is not issued, instant messenger application polices cannot be enforced.

Command Modes

cfg-appfw-policy-aim configuration

cfg-appfw-policy-ymsgr configuration

cfg-appfw-policy-msnmsgr configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

The **server** command helps the instant messenger application engine to recognize the port-hopping instant messenger traffic and to enforce the security policy for that instant messenger application; thus, if this command is not issued, the security policy cannot be enforced if IM applications use port-hopping techniques.

To deploy IM traffic enforcement policies effectively, it is recommended that you issue the appropriate **server** command.

Note If a router cannot identify a packet as belonging to a particular instant messenger policy, the corresponding policy cannot be enforced.

To configure more than one set of servers, you can issue the **server** command multiple times within an instant messenger's application policy. Multiple entries are treated cumulatively.

The server name Command

The server command (with the **name** keyword) internally resolves the DNS name of the server. This command sends DNS queries multiple times to gather all possible IP addresses for the IM servers, which return different IP addresses at different times in response to DNS queries of the same names. It uses the Time to Live (TTL) field found in DNS responses to refresh its cache. After a certain period, the DNS cache in IM applications stabilize. It is recommended that you allow a couple of minutes for the DNS cache to populate with the IM server IP addresses before the IM traffic reaches the Cisco IOS firewall. All existing IM application connections are not subjected to IM policy enforcement.

Denying Access to a Particular Instant Messenger Application

You can deny traffic to a particular instant messenger application in one of the following ways:

- Issue the **server deny** command and list all the server names and IP addresses to which you want to deny access.

Note The first option is the preferred method because it performs slightly better than the second option.

- Issue the **server permit** command and list all the server names and IP addresses that you want inspected; thereafter, issue the **service default reset** command, which will deny access to all services.
- Issue **server deny** command to block access to any site given its DNS name. For example, to block all access to a gambling site, you can configure **server deny name www.noaccess.com**.

Examples

The following example shows to configure application policy "my-im-policy," which allows text-chat for Yahoo! instant messenger users and blocks instant messenger traffic for all other users:

```
appfw policy-name my-im-policy
 application http
  port-misuse im reset
!
 application im yahoo
  server permit name scs.msg.yahoo.com
  server permit name scsa.msg.yahoo.com
  server permit name scsb.msg.yahoo.com
  server permit name scsc.msg.yahoo.com
  service text-chat action allow
  service default action reset
!
 application im aol
  server deny name login.cat.aol.com
!
```

```
 application im msn
  server deny name messenger.hotmail.com
!
ip inspect name test appfw my-im-policy

interface FastEthernet0/0
 description Inside interface
 ip inspect test in
```

Related Commands

Command	Description
service	Specifies an action when a specific service is detected in the instant messenger traffic.

server

To associate a Diameter server with a Diameter authentication, authorization, and accounting (AAA) server group, use the **server** command in Diameter server group configuration submode. To remove a server from the server group, enter the **no** form of this command.

server *name*

no server *name*

Syntax Description

name	Character string used to name the Diameter server. **Note** The name specified for this command should match the name of a Diameter peer defined using the **diameter peer** command.

Command Default

No server is associated with a Diameter AAA server group.

Command Modes

Diameter server group configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

The **server** command allows you to associate a Diameter server with a Diameter server group.

Examples

The following example shows how to associate a Diameter server with a Diameter server group:

```
Router (config-sg-diameter)# server dia_peer_1
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication login	Set AAA authentication at login.
aaa authorization	Sets parameters that restrict user access to a network.
aaa group server diameter	Configures a server group for Diameter.

server (ldap)

To associate a particular Lightweight Directory Access Protocol (LDAP) server with a AAA server group, use the **server** command in LDAP server group configuration mode. To delete a server name from the LDAP server, use the **no** form of this command.

server *name*

no server *name*

Syntax Description

name	LDAP server name.

Command Default

No server name is configured in the LDAP server.

Command Modes

LDAP server group configuration (config-ldap-server)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Examples

The following example shows how to associate an LDAP server named server1 with a AAA server group:

```
Router(config)# aaa group server ldap name1
Router(config-ldap-sg)# server server1
```

Related Commands

Command	Description
ldap server	Defines an LDAP server and enters LDAP server configuration mode.

server (parameter-map)

To configure a set of Domain Name System (DNS) servers with which a given instant messenger application interacts, use the **server** command in parameter-map configuration mode. To disable the configuration, use the **no** form of this command.

server {**name** *string* [**snoop**] | **ip** {*ip-address* | **range** *ip-address-start ip-address-end*}

no server {**name** *string* [**snoop**] | **ip** {*ip-address* | **range** *ip-address-start ip-address-end*}

Syntax Description

name *string*	Specifies the name of the DNS server for which traffic will be permitted (and inspected) or denied.
snoop	(Optional) Enables DNS snooping.
ip	Indicates that at least one IP address will be listed.
ip-address	IP address of the DNS server for which traffic will be permitted (and inspected) or denied. **Note** You cannot configure network addresses that are reserved for special purposes as the server IP address. For example, IP addresses such as 0.0.0.0, 127.0.0.0, and 127.0.0.1 cannot be configured as the server IP address.
range *ip-address-start ip-address-end*	Specifies the range of DNS server IP addresses for which traffic will be permitted (and inspected) or denied.

Command Default

At least one server instance should be configured for the configured instant messenger policy to be enforced; otherwise, the parameter map will not have any definitions to enforce.

Command Modes

Parameter-map configuration (config-profile)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.4(20)T	This command was modified. The **snoop** keyword was added. Support for the I Seek You (ICQ) and Windows Messenger IM Protocols was added.

Usage Guidelines

The **server** command helps the instant messenger application engine to recognize traffic from an instant messenger and to enforce the configured policy for that instant messenger application.

Before you can issue the **server** command, you must issue the **parameter-map type** command, which allows you to specify parameters that control the behavior of actions and match criteria specified under a policy map and a class map, respectively.

Note To enable name resolution, you must also enable the **ip domain name** and **ip name-server** commands.

To configure more than one set of servers, you can configure the **server** command multiple times within an instant messenger's parameter map. Multiple entries are treated cumulatively.

DNS Snooping

In Cisco IOS Release 12.4(20)T, users can enable DNS snooping on an access router to easily obtain address names. When DNS snooping is enabled, the Cisco IOS firewall that is running on the access router can "snoop" the DNS responses that are going through the router. The firewall can obtain the necessary addresses from the DNS responses because the DNS inspection engine decodes the DNS response packets and returns a list of addresses to the address database.

When using DNS snooping, network administrators no longer have to give a complete address, such as abcd.example1.example.com; instead, they can specify a partial address with a "wildcard character," such as *.example1.example.com.

Examples

The following example shows how to configure an IM-based firewall policy. In this example, all Yahoo Messenger and AOL traffic is allowed to pass through, while all MSN Messenger traffic is blocked. Also, parameter maps are defined to control all Yahoo Messenger and AOL traffic on a more granular level.

```
! Define Layer 7 class-maps.
class-map type inspect ymsgr match-any l7-cmap-ymsgr
 match service text-chat
!
class-map type inspect aol match-any l7-cmap-aol
 match service text-chat
 match service any
!
! Define Layer 7 policy-maps.
policy-map type inspect im l7-pmap-ymsgr
 class-type inspect ymsgr l7-cmap-ymsgr
  allow
  alarm
!
!
policy-map type inspect im l7-pmap-aol
 class-type inspect aol l7-cmap-aol
  allow
  alarm
!
!
! Define parameter map.
parameter-map type protocol-info ymsgr
 server name sdsc.msg.yahoo.com
 server ip 10.1.1.1
!
parameter-map type protocol-info aol
 server name sdsc.msg.aol.com
 server ip 172.16.1.1.
```

The following example shows how to configure an access router to block ICQ and Yahoo IM applications while allowing only text chat with Windows Messenger. In this example, snooping is enabled to obtain addressess for all IM applications.

```
! Define the servers for ICQ.
parameter-map type protocol-info icq-servers
 server name *.icq.com snoop
 server name oam-d09a.blue.aol.com

! Define the servers for Windows Messenger.
parameter-map type protocol-info winmsgr-servers
```

```
 server name messenger.msn.com snoop

! Define servers for yahoo.
parameter-map type protocol-info yahoo-servers
 server name scs*.msg.yahoo.com snoop
 server name c*.msg.yahoo.com snoop

! Define class-map to match ICQ traffic.
class-map type inspect icq-traffic
 match protocol icq icq-servers

! Define class-map to match windows Messenger traffic.
class-map type inspect winmsgr-traffic
 match protocol winmsgr winmsgr-servers
!

! Define class-map to match text-chat for windows messenger.
class-map type inspect winmsgr winmsgr-textchat
 match service text-chat
!

Define class-map to match default service
class-map type inspect winmsgr winmsgr-defaultservice
 match service any
!

! Define a Layer 7 IM policy-map to permit text-chat and block everything else.
policy-map type inspect im im-policy
 class type inspect winmsgr winmsgr-textchat
  allow
  !
 class type inspect winmsgr winmsgr-defaultservice
  reset
  !
!

! Define the Layer 4 policy to block ICQ and Yahoo Messenger and allow yahoo text-chat
! with Windows Messenger
policy-map type inspect firewall-policy
 class type inspect winmsgr-traffic
  inspect
  service-policy type inspect im im-policy
  !
 class type inspect icq-traffic
  drop
  !
 class type inspect yahoo-traffic
  drop
```

Related Commands

Command	Description
ip domain lookup	Enables the IP DNS-based hostname-to-address translation.
ip domain name	Defines a default domain name that the Cisco IOS software uses to complete unqualified hostnames (names without a dotted-decimal domain name).
ip name-server	Specifies the address of one or more name servers to be used for name and address resolution.
parameter-map type	Creates or modifies a parameter map.

server (RADIUS)

To configure the IP address of the RADIUS server for the group server, use the **server** command in server-group configuration mode. To remove the associated server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

server *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]

no server *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]

Syntax Description

ip-address	IP address of the RADIUS server host.
auth-port *port-number*	(Optional) Specifies the User Datagram Protocol (UDP) destination port for authentication requests. The port-number argument specifies the port number for authentication requests. The host is not used for authentication if this value is set to 0.
acct-port *port-number*	(Optional) Specifies the UDP destination port for accounting requests. The port number argument specifies the port number for accounting requests. The host is not used for accounting services if this value is set to 0.

Defaults

If no port attributes are defined, the defaults are as follows:

- Authentication port: 1645
- Accounting port: 1646

Command Modes

Server-group configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(7)T	The following new keywords/arguments were added: • **auth-port** *port-number* • **acct-port** *port-number*
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **server** command to associate a particular server with a defined group server. There are two different ways in which you can identify a server, depending on the way you want to offer AAA services. You can identify the server simply by using its IP address, or you can identify multiple host instances or entries using the optional **auth-port** and **acct-port** keywords.

When you use the optional keywords, the network access server identifies RADIUS security servers and host instances associated with a group server on the basis of their IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS host entries providing a specific AAA service. If two different host entries on the same RADIUS server are configured for the same service—for example, accounting—the second host entry configured acts as failover backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server will try the second host entry configured on the same device for accounting services. (The RADIUS host entries will be tried in the order they are configured.)

Examples

Configuring Multiple Entries for the Same Server IP Address

The following example shows the network access server configured to recognize several RADIUS host entries with the same IP address. Two different host entries on the same RADIUS server are configured for the same services—authentication and accounting. The second host entry configured acts as fail-over backup to the first one. (The RADIUS host entries are tried in the order in which they are configured.)

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default radius
! The next set of commands configures multiple host entries for the same IP address.
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.20.0.1 auth-port 2000 acct-port 2000
```

Configuring Multiple Entries Using AAA Group Servers

In this example, the network access server is configured to recognize two different RADIUS group servers. One of these groups, group1, has two different host entries on the same RADIUS server configured for the same services. The second host entry configured acts as failover backup to the first one.

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default group group1
! The following commands define the group1 RADIUS group server and associates servers
! with it.
aaa group server radius group1
   server 172.20.0.1 auth-port 1000 acct-port 1001
! The following commands define the group2 RADIUS group server and associates servers
! with it.
aaa group server radius group2
   server 172.20.0.1 auth-port 2000 acct-port 2001
! The following set of commands configures the RADIUS attributes for each host entry
! associated with one of the defined group servers.
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.31.0.1 auth-port 1645 acct-port 1646
```

Related Commands

Command	Description
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.

server (TACACS+)

To configure the IP address of the TACACS+ server for the group server, use the **server** command in TACACS+ group server configuration mode. To remove the IP address of the RADIUS server, use the **no** form of this command.

server *ip-address*

no server *ip-address*

Syntax Description

ip-address	IP address of the selected server.

Defaults

No default behavior or values.

Command Modes

TACACS+ group server configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You must configure the **aaa group server tacacs** command before configuring this command.

Enter the **server** command to specify the IP address of the TACACS+ server. Also configure a matching **tacacs-server host** entry in the global list. If there is no response from the first host entry, the next host entry is tried.

Examples

The following example shows server host entries configured for the RADIUS server:

```
aaa new-model
aaa authentication ppp default group g1
aaa group server tacacs+ g1
 server 10.0.0.1
 server 10.2.0.1
tacacs-server host 10.0.0.1
tacacs-server host 10.2.0.1
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.

Command	Description
aaa server group	Groups different server hosts into distinct lists and distinct methods.
tacacs-server host	Specifies a RADIUS server host.

server address ipv4

To specify the address of the server that a Group Domain of Interpretation (GDOI) group is trying to reach, use the **server address ipv4** command in GDOI group configuration mode. To disable the address, use the **no** form of this command.

server address ipv4 {*address* | *hostname*}

no server address ipv4 {*address* | *hostname*}

Syntax Description

address	IP address of the server.
hostname	Hostname of the server.

Command Default

None

Command Modes

GDOI group configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The **server address ipv4** command can be used only on a group member. This command must be specified or the group configuration on the group member is not complete.

Examples

The following example shows that the GDOI group is trying to reach the server with the IP address "10.34.255.57":

```
server address ipv4 10.34.255.57
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

server local

To designate a device as a Group Domain of Interpretation (GDOI) key server and enter GDOI local server configuration mode, use the **server local** command in GDOI group configuration mode. To remove a device as a key server, use the **no** form of this command.

server local

no server local

Syntax Description

This command has no arguments or keywords.

Command Default

A device is not designated as a GDOI key server.

Command Modes

GDOI group configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command is used on the key server to specify the key server policy that will be downloaded to the group members that are registered with the key server.

Examples

The following example shows that the device has been designated as a GDOI key server:

```
server local
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.

server vendor

To specify the URL filtering server, use the **server vendor** command in URL parameter-map configuration mode. To remove a server from the configuration, use the **no** form of this command.

server vendor {**n2h2** | **websense**} {*ip-address* | *hostname*} [**outside**] [**port** *port-number*] [**retrans** *retransmission-count*] [**timeout** *seconds*]

no server vendor {**n2h2** | **websense**} {*ip-address* | *hostname*} [**outside**] [**port** *port-number*] [**retrans** *retransmission-count*] [**timeout** *seconds*]

Syntax Description

n2h2	Specifies the N2H2 server.
websense	Specifies the Websense server.
ip-address	IP address of the URL filtering server that you want to configure.
hostname	Hostname of the URL filtering server that you want to configure.
outside	(Optional) Specifies that the vendor server is on the outside network.
port *port-number*	(Optional) Specifies the port number on which the vendor server listens. The range is from 1 to 65535. The default port for the Websense vendor is 15868 and the N2H2 vendor is 4005.
retrans *retransmission-count*	(Optional) Specifies the number of times the Cisco IOS firewall will retransmit the request when a response does not arrive for the request. The range is from 1 to 10. The default value is 2.
timeout *seconds*	(Optional) Specifies the length of time, in seconds, that the Cisco IOS firewall will wait for a response from the vendor server. The range is from 1 to 300. The default value is 6.

Command Default

No URL filtering is performed.

Command Modes

URL parameter-map configuration (config-profile)

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Use the **server vendor** command to specify the URL filtering server. If there is no server, there can be no URL filtering.

When you are creating a URL filter parameter map, you can use the **server vendor** command after entering the **parameter-map type urlfilter** command. For more detailed information about creating a parameter map, see the **parameter-map type urlfilter** command.

Use the **server vendor** command to configure a Websense or N2H2 server, which will interact with the Cisco IOS firewall to filter HTTP requests on the basis of a specified policy—global filtering, user- or group-based filtering, keyword-based filtering, category-based filtering, or customized filtering.

If the firewall has not received a response from the vendor server within the time specified in the **timeout** *seconds* keyword and argument, the firewall checks the **retrans** *retransmission-count* keyword and argument configured for the vendor server. If the firewall has not exceeded the maximum retransmit tries allowed, it resends the HTTP lookup request. If the firewall has exceeded the maximum retransmit tries allowed, it deletes the outstanding request from the queue and checks the value specified in the **allow-mode** command. The firewall forwards the request if the allow mode is on; otherwise, it drops the request.

By default, URL lookup requests that are made to the vendor server contain nonnatted client IP addresses because the vendor server is deployed on the inside network. The **outside** keyword allows the vendor server to be deployed on the outside network. Cisco IOS software sends, in the URL lookup request, the client's IP address that has undergone network address translation (NAT).

Primary and Secondary Servers

When you configure multiple vendor servers, the Cisco IOS firewall uses only one server at a time—the primary server; all other servers are called secondary servers. When the primary server becomes unavailable for any reason, it becomes a secondary server and one of the secondary servers becomes the primary server.

A firewall marks a primary server as down when sending a request to or receiving a response from the server fails. When a primary server goes down, the system goes to the beginning of the configured servers list and tries to activate the first server on the list. If the first server on the list is unavailable, it tries the second server on the list; the system keeps trying to activate a server until it is successful or until it reaches the end of the server list. If the system reaches the end of the server list, it sets a flag indicating that all of the servers are down, and it enters allow mode. When allow mode is on, HTTP traffic is permitted.

Examples

The following example shows how to specify the N2H2 vendor server for URL filtering:

```
parameter-map type urlfilter u1
 server vendor n2h2 10.193.64.22 port 3128 outside
```

Related Commands

Command	Description
allow-mode	Turns the default mode of the filtering algorithm on or off.
ip urlfilter server vendor	Configures a vendor server for URL filtering.
max-request	Specifies the maximum number of outstanding requests that can exist at any given time.
parameter-map type urlfilter	Creates a parameter map that will hold parameters pertaining to the URL filter.

server-private (RADIUS)

To configure the IP address of the private RADIUS server for the group server, use the **server-private** command in server-group configuration mode. To remove the associated private server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

server-private *ip-address* [**auth-port** *port-number* | **acct-port** *port-number*] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

no server-private *ip-address* [**auth-port** *port-number* | **acct-port** *port-number*] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

Syntax Description

ip-address	IP address of the private RADIUS server host.
auth-port *port-number*	(Optional) User Datagram Protocol (UDP) destination port for authentication requests. The default value is 1645.
acct-port *port-number*	Optional) UDP destination port for accounting requests. The default value is 1646.
non-standard	(Optional) RADIUS server is using vendor-proprietary RADIUS attributes.
timeout *seconds*	(Optional) Time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the **radius-server timeout** command. If no timeout value is specified, the global value is used.
retransmit *retries*	(Optional) Number of times a RADIUS request is resent to a server, if that server is not responding or responding slowly. This setting overrides the global setting of the **radius-server retransmit** command.
key *string*	(Optional) Authentication and encryption key used between the router and the RADIUS daemon running on the RADIUS server. This key overrides the global setting of the **radius-server key** command. If no key string is specified, the global value is used.

Defaults

If server-private parameters are not specified, global configurations will be used; if global configurations are not specified, default values will be used.

Command Modes

Server-group configuration

Command History

Release	Modification
12.2(1)DX	This command was introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Release	Modification
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **server-private** command to associate a particular private server with a defined server group. To prevent possible overlapping of private addresses between Virtual Route Forwardings (VRFs), private servers (servers with private addresses) can be defined within the server group and remain hidden from other groups, while the servers in the global pool (default "radius" server group) can still be referred to by IP addresses and port numbers. Thus, the list of servers in server groups includes references to the hosts in the global configuration and the definitions of private servers.

Note If the **radius-server directed-request** command is configured, then a private RADIUS server cannot be used as the group server by configuring the **server-private** (RADIUS) command.

Examples

The following example shows how to define the sg_water RADIUS group server and associate private servers with it:

```
aaa group server radius sg_water
 server-private 10.1.1.1 timeout 5 retransmit 3 key xyz
 server-private 10.2.2.2 timeout 5 retransmit 3 key xyz
```

Related Commands

Command	Description
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.
radius-server directed-request	Allows users logging into a Cisco network access server (NAS) to select a RADIUS server for authentication.

server-private (TACACS+)

To configure the IP address of the private TACACS+ server for the group server, use the **server-private** command in server-group configuration mode. To remove the associated private server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

server-private {*ip-address* | *name*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] *string*]

no server-private

Syntax Description

ip-address	IP address of the private RADIUS or TACACS+ server host.
name	Name of the private RADIUS or TACACS+ server host.
nat	(Optional) Port Network Address Translation (NAT) address of the remote device. This address is sent to the TACACS+ server.
single-connection	(Optional) Maintains a single open connection between the router and the TACACS+ server.
port *port-number*	(Optional) Specifies a server port number. This option overrides the default, which is port 49.
timeout *seconds*	(Optional) Specifies a timeout value. This value overrides the global timeout value set with the **tacacs-server timeout** command for this server only.
key [**0**	**7**]	(Optional) Specifies an authentication and encryption key. This key must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the global **tacacs-server key** command for this server only. • If no number or 0 is entered, the string that is entered is considered to be plain text. If 7 is entered, the string that is entered is considered to be encrypted text.
string	(Optional) Character string specifying the authentication and encryption key.

Command Default

If server-private parameters are not specified, global configurations will be used; if global configurations are not specified, default values will be used.

Command Modes

Server-group configuration (server-group)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(33)SRA1	This command was integrated into Cisco IOS Release 12.2(33)SRA1.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(54)SG	This command was integrated into Cisco IOS Release 12.2(54)SG.

Usage Guidelines

Use the **server-private** command to associate a particular private server with a defined server group. To prevent possible overlapping of private addresses between virtual route forwardings (VRFs), private servers (servers with private addresses) can be defined within the server group and remain hidden from other groups, while the servers in the global pool (default "TACACS+" server group) can still be referred to by IP addresses and port numbers. Thus, the list of servers in server groups includes references to the hosts in the global configuration and the definitions of private servers.

Examples

The following example shows how to define the tacacs1 TACACS+ group server and associate private servers with it:

```
aaa group server tacacs+ tacacs1
    server-private 10.1.1.1 port 19 key cisco

  ip vrf cisco
   rd 100:1

  interface Loopback0
   ip address 10.0.0.2 255.0.0.0
   ip vrf forwarding cisco
```

Related Commands

Command	Description
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
ip tacacs source-interface	Uses the IP address of a specified interface for all outgoing TACACS+ packets.
ip vrf forwarding (server-group)	Configures the VRF reference of an AAA RADIUS or TACACS+ server group.
tacacs-server host	Specifies a TACACS+ server host.

server-key

To configure the RADIUS key to be shared between a device and RADIUS clients, use the **server-key** command in dynamic authorization local server configuration mode. To remove this configuration, use the **no** form of this command.

server-key [**0** | **7**] *word*

no server-key [**0** | **7**] *word*

Syntax Description

0	(Optional) An unencrypted key will follow.
7	(Optional) A hidden key will follow.
word	Unencrypted server key.

Command Default

A server key is not configured.

Command Modes

Dynamic authorization local server configuration (config-locsvr-da-radius)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

A device (such as a router) can be configured to allow an external policy server to dynamically send updates to the router. This functionality is facilitated by the CoA RADIUS extension. CoA introduced peer-to-peer capability to RADIUS, enabling a router and external policy server each to act as a RADIUS client and server. Use the **server-key** command to configure the key to be shared between the Intelligent Services Gateway (ISG) and RADIUS clients.

Examples

The following example configures “cisco” as the shared server key:

```
aaa server radius dynamic-author
 client 10.0.0.1
 server-key cisco
```

Related Commands

Command	Description
aaa server radius dynamic-author	Configures a device as a AAA server to facilitate interaction with an external policy server.

service action

To specify an action when a specific service is detected in the instant messenger traffic, use the **service action** command in the appropriate configuration mode. To disable or change a specified action, use the **no** form of this command.

service {**default** | **text-chat**} **action** {**allow** [**alarm**] | **reset** [**alarm**] | **alarm**}

no service {**default** | **text-chat**} **action** {**allow** [**alarm**] | **reset** [**alarm**] | **alarm**}

Syntax Description

default	Matches all services that are not explicitly configured under the application. **Note** It is recommended that when an IM application is allowed, always specify the default option for an IM application.
text-chat	Controls the text-based chat service that is provided by instant messenger applications.
action	Indicates that a specific action is to follow.
allow	Allows a specific service.
reset	Blocks the service specified in the configuration. If the **default** option is being used, only services for which a specific action has been identified are allowed; all other services are denied.
alarm	Generates an alarm message when the specified service is encountered over the connection.

Command Default

If the command is not configured, the default is **service default action reset**.

Command Modes

cfg-appfw-policy-aim configuration

cfg-appfw-policy-ymsgr configuration

cfg-appfw-policy-msnmsgr configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

When the **reset** keyword is used, the connection is reset if TCP is used, and the packet is dropped if UDP is used. When dropping a packet from a UDP connection, the session will not be immediately deleted; instead, the session will time out to prevent additional sessions from being immediately created.

The **alarm** keyword can be specified alone or with the **allow** or **reset** keywords; however, the **allow** or **reset** keywords are mutually exclusive.

Examples

The following example shows to configure application policy “my-im-policy,” which allows text-chat for Yahoo! instant messenger users and blocks instant messenger traffic for all other users:

```
appfw policy-name my-im-policy
 application http
  port-misuse im reset
!
 application im yahoo
  server permit name scs.msg.yahoo.com
  server permit name scsa.msg.yahoo.com
  server permit name scsb.msg.yahoo.com
  server permit name scsc.msg.yahoo.com
  service text-chat action allow
  service default action reset
!
 application im aol
  server deny name login.user1.aol.com
!
 application im msn
  server deny name messenger.hotmail.com
!
ip inspect name test appfw my-im-policy

interface FastEthernet0/0
 description Inside interface
 ip inspect test in
```

service password-encryption

To encrypt passwords, use the **service password-encryption** command in global configuration mode. To restore the default, use the **no** form of this command.

service password-encryption

no service password-encryption

Syntax Description

This command has no arguments or keywords.

Command Default

No passwords are encrypted.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The actual encryption process occurs when the current configuration is written or when a password is configured. Password encryption is applied to all passwords, including username passwords, authentication key passwords, the privileged command password, console and virtual terminal line access passwords, and Border Gateway Protocol neighbor passwords. This command is primarily useful for keeping unauthorized individuals from viewing your password in your configuration file.

When password encryption is enabled, the encrypted form of the passwords is displayed when a **more system:running-config** command is entered.

Caution This command does not provide a high level of network security. If you use this command, you should also take additional network security measures.

Note You cannot recover a lost encrypted password. You must clear NVRAM and set a new password.

Examples

The following example causes password encryption to take place:

```
service password-encryption
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
key-string (authentication)	Specifies the authentication string for a key.
neighbor password	Enables MD5 authentication on a TCP connection between two BGP peers.

service password-recovery

To enable password recovery capability, use the **service password-recovery** command in global configuration mode. To disable password recovery capability, use the **no service password-recovery** command.

service password-recovery

no service password-recovery

Syntax Description

This command has no arguments or keywords.

Defaults

Password recovery capability is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)YA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Usage Guidelines

Note This command is not available on all platforms. Use Feature Navigator to ensure that it is available on your platform.

If you plan to disable the password recovery capability with the the **no service password-recovery** command, we recommend that you save a copy of the system configuration file in a location away from the switch or router. If you are using a switch that is operating in VTP transparent mode, we recommend that you also save a copy of the vlan.dat file in a location away from the switch.

Caution Entering the **no service password-recovery** command at the command line disables password recovery. Always disable this command before downgrading to an image that does not support password recovery capability, because you cannot recover the password after the downgrade.

The configuration register boot bit must be enabled so that there is no way to break into ROMMON when this command is configured. Cisco IOS software should prevent the user from configuring the boot field in the config register.

Bit 6, which ignores the startup configuration, and bit 8, which enables a break should be set.

The Break key should be disabled while the router is booting up and disabled in Cisco IOS software when this feature is enabled.

It may be necessary to use the **config-register** global configuration command to set the configuration register to autoboot before entering the **no service password-recovery** command. The last line of the **show version** EXEC command displays the configuration register setting. Use the **show version** EXEC command to obtain the current configuration register value, configure the router to autoboot with the **config-register** command if necessary, then enter the **no service password-recovery** command.

Once disabled, the following configuration register values are invalid for the **no service password-recovery** command:

- 0x0
- 0x2002 (bit 8 restriction)
- 0x0040 (bit 6)
- 0x8000 (bit 15)

Catalyst Switch Operation

Use the **service password-recovery** command to reenable the password-recovery mechanism (the default). This mechanism allows a user with physical access to the switch to hold down the Mode button and interrupt the boot process while the switch is powering up and to assign a new password. Use the **no** form of this command to disable the password-recovery capability.

When the password-recovery mechanism is disabled, interrupting the boot process is allowed only if the user agrees to set the system back to the default configuration. Use the **show version** EXEC command to verify if password recovery is enabled or disabled on a switch.

The **service password-recovery** command is valid only on Catalyst 3550 Fast Ethernet switches; it is not available for Gigabit Ethernet switches.

Examples

Router Configuration Examples

The following example shows how to obtain the configuration register setting (which in this example is set to autoboot), disable the password-recovery capability, and then verify that the configuration persists through a system reload. The **noconfirm** keyword prevents a confirmation prompt from interrupting the booting process.

```
Router# show version

Cisco Internetwork Operating System Software
IOS (tm) 5300 Software (C7200-P-M), Version 12.3(8)YA, RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Wed 05-Mar-03 10:16 by xxx
Image text-base: 0x60008954, data-base: 0x61964000

ROM: System Bootstrap, Version 12.3(8)YA, RELEASE SOFTWARE (fc1)
BOOTLDR: 7200 Software (C7200-KBOOT-M), Version 12.3(8)YA, RELEASE SOFTWARE (fc1)

Router uptime is 10 minutes
System returned to ROM by reload at 16:28:11 UTC Thu Mar 6 2003
.
.
.
125440K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
8192K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x2012

Router# configure terminal

Router(config)# no service password-recovery noconfirm
```

```
WARNING:
Executing this command will disable the password recovery mechanism.
Do not execute this command without another plan for password recovery.
Are you sure you want to continue? [yes/no]: yes
.
.
.
Router(config)# exit
Router#
Router# reload

Proceed with reload? [confirm] yes

00:01:54: %SYS-5-RELOAD: Reload requested
System Bootstrap, 12.3(8)YA...
Copyright (c) 1994-2004 by cisco Systems, Inc.
C7400 platform with 262144 Kbytes of main memory

PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
.
.
.
```

The following example shows what happens when a break is confirmed and when a break is not confirmed.

Confirmed Break

```
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
program load complete, entry point: 0x80013000, size: 0x8396a8
Self decompressing the image :

################################################################################################
################################## [OK] !The 5-second window starts.

telnet> send break

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR
sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software, C831 Software (C831-K9O3SY6-M), Version 12.3(8)YA
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Fri 13-Aug-04 03:21
Image text-base: 0x80013200, data-base: 0x81020514

PASSWORD RECOVERY IS DISABLED.
Do you want to reset the router to factory default configuration and proceed [y/n]?
!The user enters "y" here.

Reset router configuration to factory default.

This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
```

```
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

Cisco C831 (MPC857DSL) processor (revision 0x00) with 46695K/2457K bytes of memory.
Processor board ID 0000 (1314672220), with hardware revision 0000 CPU rev number 7
3 Ethernet interfaces
4 FastEthernet interfaces
128K bytes of NVRAM
24576K bytes of processor board System flash (Read/Write)
2048K bytes of processor board Web flash (Read/Write)

         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no
!Start up config is erased.

SETUP: new interface FastEthernet1 placed in "up" state
SETUP: new interface FastEthernet2 placed in "up" state
SETUP: new interface FastEthernet3 placed in "up" state
SETUP: new interface FastEthernet4 placed in "up" state

Press RETURN to get started!

Router> enable
Router# show startup configuration

startup-config is not present

Router# show running-config | incl service

no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption !The "no service password-recovery" is disabled.

==========================================================================================
```

Unconfirmed Break

```
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED

telnet> send break

program load complete, entry point: 0x80013000, size: 0x8396a8
Self decompressing the image :
########################################################################################
########################################################################## [OK]

telnet> send break

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR
sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
```

```
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software, C831 Software (C831-K9O3SY6-M), Version 12.3(8)YA
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Fri 13-Aug-04 03:21
Image text-base: 0x80013200, data-base: 0x81020514

PASSWORD RECOVERY IS DISABLED.
Do you want to reset the router to factory default configuration and proceed [y/n]?
!The user enters "n" here.

This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption.
Importers, exporters, distributors and users are responsible for compliance with U.S. and
local country laws. By using this product you agree to comply with applicable laws and
regulations. If you are unable to comply with U.S. and local laws, return this product
immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

Cisco C831 (MPC857DSL) processor (revision 0x00) with 46695K/2457K bytes of memory.
Processor board ID 0000 (1314672220), with hardware revision 0000 CPU rev number 7
3 Ethernet interfaces
4 FastEthernet interfaces
128K bytes of NVRAM
24576K bytes of processor board System flash (Read/Write)
2048K bytes of processor board Web flash (Read/Write)

Press RETURN to get started! !The Cisco IOS software boots as if it is not interrupted.

Router> enable

Router# show startup configuration

Using 984 out of 131072 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
no service password-recovery
!
hostname Router
!
boot-start-marker
boot-end-marker
!
memory-size iomem 5
!
no aaa new-model
ip subnet-zero
!
ip ips po max-events 100
no ftp-server write-enable
!
interface Ethernet0
```

```
 no ip address
 shutdown
!
interface Ethernet1
 no ip address
 shutdown
 duplex auto
!
interface Ethernet2
 no ip address
 shutdown
!
interface FastEthernet1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet2
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet3
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet4
 no ip address
 duplex auto
 speed auto
!
ip classless
!
ip http server
no ip http secure-server
!
control-plane
!
line con 0
 no modem enable
 transport preferred all
 transport output all
line aux 0
line vty 0 4
!
scheduler max-task-time 5000
end

Router# show running-configuration | incl service

no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
no service password-recovery
```

Configuration Register Messages Example

The **no service password-recovery** command expects the router configuration register to be configured to autoboot. If the configuration register is set to something other than to autoboot before the **no service password-recovery** command is entered, you will see a prompt like the one shown in the following example asking you to use the **config-register** global configuration command to change the setting.

```
Router(config)# no service password-recovery

Please setup auto boot using config-register first.
```

Note To avoid any unintended result due to the behavior of this command, use the **show version** EXEC command to obtain the current configuration register value. If not set to autoboot, you will need to configure the router to autoboot with the **config-register** command before entering the **no service password-recovery** command.

Once password recovery is disabled, you will not be able set bit pattern 0x40, 0x8000 or set the value to 0x0 to disable autoboot. The following example shows the messages displayed when invalid configuration register settings are attempted on a router with password recovery disabled.

```
Router(config)# config-register 0x2143

Password recovery is disabled, cannot enable diag or ignore configuration.
```

The command will reset the invalid bit pattern and continue to allow modification of nonrelated bit patterns. The configuration register value will be reset to 0x3 at the next system reload, which can be verified by checking the last line of the **show version** command output:

```
Configuration register is 0x2012 (will be 0x3 at next reload)
```

Catalyst Switch Example

The following example shows how to disable password recovery on a switch so that a user can only reset a password by agreeing to return to the default configuration:

```
Switch(config)# no service-password recovery
Switch(config)# exit
```

To use the password-recovery procedure, a user with physical access to the switch holds down the Mode button while the unit powers up and for a second or two after the LED above port 1X goes off. When the button is released, the system continues with initialization. If the password-recovery mechanism is disabled, the following message is displayed:

```
The password-recovery mechanism has been triggered, but is currently disabled. Access to
the boot loader prompt through the password-recovery mechanism is disallowed at this
point. However, if you agree to let the system be reset back to the default system
configuration, access to the boot loader prompt can still be allowed.

Would you like to reset the system back to the default configuration (y/n)?
```

If you choose not to reset the system back to the default configuration, the normal boot process continues, as if the Mode button had not been pressed. If you choose to reset the system back to the default configuration, the configuration file in flash memory is deleted and the VLAN database file, flash:vlan.dat (if present), is deleted.

The following is sample output from the **show version** privileged EXEC command on a switch when password recovery is disabled:

```
Switch# show version

Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-I9Q3L2-M), Version 12.3(8)YA, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Wed 24-Oct-01 06:20 by xxx
Image text-base: 0x00003000, data-base: 0x004C1864

ROM: Bootstrap program is C3550 boot loader

flam-1-6 uptime is 1 week, 6 days, 3 hours, 59 minutes
System returned to ROM by power-on

Cisco WS-C3550-48 (PowerPC) processor with 65526K/8192K bytes of memory.
Last reset from warm-reset
Running Layer2 Switching Only Image

Ethernet-controller 1 has 12 Fast Ethernet/IEEE 802.3 interfaces

Ethernet-controller 2 has 12 Fast Ethernet/IEEE 802.3 interfaces

Ethernet-controller 3 has 12 Fast Ethernet/IEEE 802.3 interfaces

Ethernet-controller 4 has 12 Fast Ethernet/IEEE 802.3 interfaces

Ethernet-controller 5 has 1 Gigabit Ethernet/IEEE 802.3 interface

Ethernet-controller 6 has 1 Gigabit Ethernet/IEEE 802.3 interface

48 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

The password-recovery mechanism is disabled.
32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: AA:00:0B:2B:02:00
Configuration register is 0x10F
```

Related Commands

Command	Description
config-register	Changes the configuration register settings.
show version	Displays version information for the hardware and firmware.

service-module ids bootmode

To enter failsafe or normal boot mode for a Cisco Intrusion Prevention System (IPS) network module (also referred to as the Cisco Intrusion Detection System [IDS] network module and as the NME-IPS), use the **service-module ids bootmode** command in privileged EXEC mode.

service-module ids *slot*/*port* **bootmode** {**failsafe** | **normal**}

Syntax Description

slot/	Number of the router chassis slot for the network module. The slash mark (/) is required between the *slot* argument and the *port* argument.
port	Port number of the network module. For Cisco IPS network modules, always use 0.
failsafe	Enters IDS failsafe boot mode on a Cisco IPS network module.
normal	Enters IDS normal boot mode on a Cisco IPS network module.

Defaults

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

If a confirmation prompt is displayed, press **Enter** to confirm the action, or press **n** to cancel.

Examples

The following example enters the IDS failsafe boot mode on the Cisco IPS network module in slot 1:

```
Router# service-module ids 1/0 bootmode failsafe
```

The following example enters the IDS failsafe boot mode on the Cisco IPS network module in slot 1:

```
Router# service-module ids 1/0 bootmode normal
```

Related Commands

Command	Description
ids-service-module monitoring	Enables IDS monitoring on a specified interface.

service-module ids heartbeat-reset

To prevent the Cisco IOS software from rebooting the Cisco Intrusion Prevention System (IPS) network module (also referred to as the Cisco Intrusion Detection System [IDS] network module and as the NME-IPS), when the heartbeat is lost, use the **service-module ids heartbeat-reset** command in privileged EXEC mode.

service-module ids *slot*/*port* **heartbeat-reset** {**enable** | **disable**}

Syntax Description

slot/	Number of the router chassis slot for the network module. The slash mark (/) is required between the *slot* argument and the *port* argument.
port	Port number of the network module. For Cisco IPS network modules, always use 0.
enable	Enables IDS heartbeat on a Cisco IPS network module.
disable	Disables IDS heartbeat on a Cisco IPS network module.

Defaults

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

When the Cisco IPS network module, or NME-IPS, is booted in failsafe mode or is undergoing an upgrade, the **service-module ids heartbeat-reset** command does not permit a reboot during the process.

When the NME-IPS heartbeat is lost, the router applies a fail-open or fail-close configuration option to the NME-IPS and stops sending traffic to the NME-IPS, and sets the NME-IPS to error state. The router performs a hardware reset on the NME-IPS and monitors the NME-IPS until the heartbeat is reestablished.

Examples

The following example disables the IDS heartbeat on the Cisco IPS network module in slot 1:

```
Router# service-module ids 1/0 heartbeat-reset disable
```

The following example enables the IDS heartbeat on the Cisco IPS network module in slot 1:

```
Router# service-module ids 1/0 heartbeat-reset enable
```

The status of the heartbeat-reset is displayed by using the **service-module ids** *slot*/*port* **status** command:

```
Router# service-module ids 0/0 status
Service Module is Cisco IDS-Sensor 0/0
Service Module supports session via TTY line 194
```

```
Service Module heartbeat-reset is enabled <=====
```

Related Commands

Command	Description
ids-service-module monitoring	Enables IDS monitoring on a specified interface.

service-policy (policy-map)

Note Effective with Cisco IOS Release 12.4(20)T, the **service-policy (policy-map)** command replaces the **service-policy inspect** command.

To attach a Layer 7 policy map to the top-level Layer 3 or Layer 4 policy map, use the **service-policy** command in policy-map-class configuration mode. To disable the attachment, use the **no** form of this command.

service-policy {**h323** | **http** | **im** | **imap** | **p2p** | **pop3** | **sip** | **smtp** | **sunrpc** | **urlfilter**} *policy-map*

no service-policy {**h323** | **http** | **im** | **imap** | **p2p** | **pop3** | **sip** | **smtp** | **sunrpc** | **urlfilter**} *policy-map*

Syntax Description

h323	Associates the class with an H.323 protocol Deep Packet Inspection (DPI).
http	Associates the class with an HTTP DPI.
im	Associates the class with an Instant Messenger (IM) protocol DPI.
imap	Associates the class with an Internet Message Access Protocol (IMAP) DPI.
p2p	Associates the class with a P2P protocol DPI.
pop3	Associates the class with a Post Office Protocol, Version 3 (POP3) DPI.
sip	Associates the class with a Session Initiation Protocol (SIP) DPI
smtp	Associates the class with an Simple Mail Transfer Protocol (SMTP) DPI.
sunrpc	Associates the class with a SUN Remote Procedure Call (SUNRPC) DPI.
urlfilter	Associates the class with a URL filter DPI.
policy-map	Name of the Layer 7 policy map.

Command Default

Disabled.

Command Modes

Policy-map-class configuration (config-pmap-c)

Command History

Release	Modification
12.4(20)T	This command was introduced. This command replaces the **service policy-inspect** command.

Usage Guidelines

The **service-policy (policy-map)** command attaches a Layer 7 policy-map to the top-level Layer 3 or Layer 4 policy map. The Layer 7 policy is a nested policy of the top-level policy, and it is called a child policy.

Examples

The following example creates a Layer 3 or Layer 4 policy called test, attaches a Layer 7 policy called p11 to that policy, and inspects H.323 traffic.

```
!
class-map type inspect match-all test
 match protocol h323
class-map type inspect h323 match-any c1
 match  message setup
!
policy-map type inspect h323 p11
 class type inspect h323 c1
  log
  rate-limit 15
policy-map type inspect test
 class type inspect test
  inspect
  service-policy h323 p11
 class class-default
  drop
!
```

Related Commands

Command	Description
policy-map type inspect	Creates a Layer 3, Layer 4 inspect type policy map or a Layer 7 application-specific inspect type policy map.

service-policy (zones)

To attach a Layer 7 policy map to a top-level policy map, use the **service-policy** command in zone-pair configuration mode. To delete a Layer 7 policy map from a top-level policy map, use the **no** form of this command.

service-policy *policy-map-name*

no service-policy *policy-map-name*

Syntax Description

policy-map-name	Name of the Layer 7 policy map to be attached to a top-level policy map.

Command Default

None

Command Modes

Zone-pair configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can enter the **service-policy** (zones) command after entering the **zone-pair** command.

Examples

The following example attaches a Layer 7 policy map to a top-level policy map:

```
policy-map type inspect p1
 class type inspect c1
  inspect
  service-policy http myhttppolicy
```

Related Commands

Command	Description
zone-pair	Creates a zone-pair.

service-policy inspect

Note Effective with Cisco IOS Release 12.4(20)T, the **service-policy inspect** command command is replaced by the **service-policy (policy-map)** command. See the **service-policy (policy-map)** command for more information.

To attach a Layer 7 policy map to the top-level Layer 3 or Layer 4 policy map, use the **service-policy inspect** command in policy-map-class configuration mode. To disable the attachment, use the **no** form of this command.

service-policy inspect {**http** | **imap** | **pop3** | **smtp** | **sunrpc**} *policy-map*

no service-policy inspect {**http** | **imap** | **pop3** | **smtp** | **sunrpc**} *policy-map*

Syntax Description

http	Associates the class with an HTTP deep inspection policy (DPI).
imap	Associates the class with an Internet Message Access Protocol (IMAP) DPI.
pop3	Associates the class with a Post Office Protocol, Version 3 (POP3) DPI.
smtp	Associates the class with an Simple Mail Transfer Protocol (SMTP) DPI.
sunrpc	Associates the class with a SUN Remote Procedure Call (SUNRPC) DPI.
policy-map	Name of the Layer 7 policy map.

Command Default

Disabled.

Command Modes

Policy-map-class configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(20)T	This command was replaced by the **service-policy (policy-map)** command.

Usage Guidelines

The **service-policy inspect** command attaches a Layer 7 policy-map to the top-level Layer 3 or Layer 4 policy map. The Layer 7 policy is considered to be a nested policy of the top-level policy, and it is called a child policy.

Examples

The following example creates a Layer 3 or Layer 4 policy map p1, attaches a Layer 7 policy called p11 to that policy, and inspects HTTP traffic.

```
policy-map type inspect p1
 class type inspect c1
  service-policy inspect http p11
```

service-policy type inspect

To attach a firewall policy map to a zone-pair, use the **service-policy type inspect** command in zone-pair configuration mode. To disable this attachment to a zone-pair, use the **no** form of this command.

service-policy type inspect *policy-map-name*

no service-policy type inspect *policy-map-name*

Syntax Description

policy-map-name	Name of the policy map. The name can be a maximum of 40 alphanumeric characters.

Command Default

None

Command Modes

Zone-pair configuration (config-sec-zone-pair)

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Use the **service-policy type inspect** command to attach a policy-map and its associated actions to a zone-pair.

Enter the command after entering the **zone-pair security** command.

Examples

The following example defines zone-pair z1-z2 and attaches the service policy p1 to the zone-pair:

```
!
zone security z1
zone security z2
!
class-map type inspect match-all c1
 match protocol tcp
policy-map type inspect p1
 class type inspect c1
  inspect
!
zone-pair security zp source z1 destination z2
 service-policy type inspect p1
!
```

Related Commands

Command	Description
zone-pair security	Creates a zone-pair.

sessions maximum

To set the maximum number of allowed sessions that can exist on a zone pair, use the **sessions maximum** command in parameter-map configuration mode. To change the number of allowed sessions, use the **no** form of this command.

sessions maximum *sessions*

no sessions maximum

Syntax Description

sessions	Maximum number of allowed sessions. Range: 1 to 2147483647.

Command Default

Default value is unlimited.

Command Modes

Parameter-map configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Use the **sessions maximum** command to limit the number of inspect sessions that match a certain class. Session limiting is activated when this parameter is configured.

This command is available only within an inspect type parameter map and takes effect only when the parameter map is associated with an inspect action in a policy.

If the **sessions maximum** command is configured, the number of established sessions on the router can be shown via the **show policy-map type inspect zone-pair** command.

Examples

The following example shows how to limit the maximum number of allowed sessions to 200 and how verify the number of established sessions:

```
parameter map type inspect abc
 sessions maximum 200

Router# show policy-map type inspect zone-pair

 Zone-pair: zp

  Service-policy inspect : test-udp

    Class-map: check-udp (match-all)
      Match: protocol udp
      Inspect
        Packet inspection statistics [process switch:fast switch]
        udp packets: [3:4454]

        Session creations since subsystem startup or last reset 92
        Current session counts (estab/half-open/terminating) [5:33:0]<---
```

```
    Maxever session counts (estab/half-open/terminating) [5:59:0]
    Last session created 00:00:06
    Last statistic reset never
    Last session creation rate 61
    Last half-open session total 33
  Police
  rate 8000 bps,1000 limit
  conformed 2327 packets, 139620 bytes; actions: transmit
  exceeded 36601 packets, 2196060 bytes; actions: drop
  conformed 6000 bps, exceed 61000 bps

Class-map: class-default (match-any)
  Match: any
  Drop (default action)
    0 packets, 0 bytes
```

Related Commands

Command	Description
parameter map type	Creates or modifies a parameter map.

sessions rate

To specify a time duration for defining the session quota, use the **sessions rate** command in parameter-map type inspect configuration mode. To disable the specified time duration, use the **no** form of this command.

sessions rate {**high** *number-of-connections* | **low** *number-of-connections* } **time** *duration*

no sessions rate {**high** | **low**}

Syntax Description

high *number-of-connections*	Number of new unestablished sessions that will cause the system to start deleting half-open sessions.
low *number-of-connections*	Number of new unestablished sessions that will cause the system to stop deleting half-open sessions.
time	Specifies the time for which the session rate limit is applied.
duration	Time duration, in seconds, for which the session rate is limited. Range is from 1 to 2147483.

Command Default

The system does not start or stop deleting half-open sessions.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced.

Usage Guidelines

You can use the **one-minute** command to define session quota within one minute. You can use the **sessions rate** command to specify the time duration in which session quota can be defined. The **sessions rate** command and the **one-minute** command are mutually exclusive. If the **one-minute** command is configured in an inspect parameter map, the **sessions rate** command is rejected, and vice versa.

Examples

The following example shows how to configure a session rate of 25 seconds:

```
Router> enable
Router# configure terminal
Router(config)# parameter-type inspect type par1
Router(config-profile)# sessions-rate high 250 time 25
```

Related Commands

Command	Description
one-minute	Defines the number of new unestablished sessions that will cause the system to start deleting half-open sessions and stop deleting half-open sessions.
parameter-map type inspect	Configures an inspect type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the inspect action.

set aggressive-mode client-endpoint

To specify the Tunnel-Client-Endpoint attribute within an Internet Security Association Key Management Protocol (ISAKMP) peer configuration, use the **set aggressive-mode client-endpoint** command in ISAKMP policy configuration mode. To remove this attribute from your configuration, use the **no** form of this command.

set aggressive-mode client-endpoint *client-endpoint*

no set aggressive-mode client-endpoint *client-endpoint*

Syntax Description

client-endpoint	One of the following identification types of the initiator end of the tunnel: • ID_IPV4 (IPV4 address) • ID_FQDN (fully qualified domain name, for example "green.cisco.com") • ID_USER_FQDN (e-mail address) The ID type is translated to the corresponding ID type in Internet Key Exchange (IKE).

Command Default

The Tunnel-Client-Endpoint attribute is not defined.

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(4)T	Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Before you can use this command, you must enable the **crypto isakmp peer** command.

To initiate an IKE aggressive mode negotiation and specify the RADIUS Tunnel-Client-Endpoint attribute, the **set aggressive-mode client-endpoint** command, along with the **set aggressive-mode password** command, *must* be configured in the ISAKMP peer policy. The Tunnel-Client-Endpoint attribute will be communicated to the server by encoding it in the appropriate IKE identity payload.

Examples

The following example shows how to initiate aggressive mode using RADIUS tunnel attributes:

```
crypto isakmp peer address 10.4.4.1
 set aggressive-mode client-endpoint user-fqdn user@cisco.com
 set aggressive-mode password cisco123
```

Related Commands

Command	Description
crypto isakmp peer	Enables an IPSec peer for IKE querying of AAA for tunnel attributes in aggressive mode.
set aggressive-mode password	Specifies the Tunnel-Password attribute within an ISAKMP peer configuration.

set aggressive-mode password

To specify the Tunnel-Password attribute within an Internet Security Association Key Management Protocol (ISAKMP) peer configuration, use the **set aggressive-mode password** command in ISAKMP policy configuration mode. To remove this attribute from your configuration, use the **no** form of this command.

set aggressive-mode password *password*

no set aggressive-mode password *password*

Syntax Description

password	Password that is used to authenticate the peer to a remote server. The tunnel password is used as the Internet Key Exchange (IKE) preshared key.

Defaults

The Tunnel-Password attribute is not defined.

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.3(2)T	This command was modified so that output shows that the preshared key is either encrypted or unencrypted.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Before you can use this command, you must enable the **crypto isakmp peer** command.

To initiate an IKE aggressive mode negotiation, the **set aggressive-mode password** command, along with the **set aggressive-mode client-endpoint** command, *must* be configured in the ISAKMP peer policy. The Tunnel-Password attribute will be used as the IKE preshared key for the aggressive mode negotiation.

Output for the **set aggressive-mode password** command will show that the preshared key is either unencrypted or encrypted. An output example for an unencrypted preshared key would be as follows:

```
set aggressive-mode password test123
```

An output example for a type 6 encrypted preshared key would be as follows:

```
set aggressive-mode password 6 DV'P[aTVWWbcgKU]T\T\QhZAAB
```

Examples

The following example shows how to initiate aggressive mode using RADIUS tunnel attributes:

```
Router (config)# crypto isakmp peer address 10.4.4.1
Router (config-isakmp-peer)# set aggressive-mode client-endpoint user-fqdn user@cisco.com
Router (config-isakmp-peer)# set aggressive-mode password cisco123
```

Related Commands

Command	Description
crypto isakmp peer	Enables an IPSec peer for IKE querying of AAA for tunnel attributes in aggressive mode.
set aggressive-mode client-endpoint	Specifies the Tunnel-Client-Endpoint attribute within an ISAKMP peer configuration.

set group

To set the Group Domain of Interpretation (GDOI) crypto map to the GDOI group that has already been defined, use the **set group** command in crypto map configuration mode. To remove the GDOI crypto map, use the **no** form of this command.

set group {*group-name*}

no set group {*group-name*}

Syntax Description

group-name	Name of the GDOI group.

Command Default

None

Command Modes

crypto map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command must be configured for the GDOI crypto map to be complete.

Note This crypto map is specifically a GDOI crypto map, that is, the crypto map must be named as a GDOI crypto map, as in this example: **crypto map test 10 gdoi**

Examples

The following example shows that the group name is “hsrp-group”:

```
set group hsrp-group
```

Related Commands

Command	Description
crypto map	Enters crypto map configuration mode and creates or modifies a crypto map entry, creates a crypto profile that provides a template for configuration of dynamically created crypto maps, indicates that the key management mechanism is GDOI, or configures a client accounting list.

set identity

To set the identity to the crypto map, use the **set identity** command in crypto map configuration mode.

set identity *name*

Syntax Description

name	Identity used to permit or restrict access for a host to a crypto map.

Defaults

If this command is not enabled, the encrypted connection does not have any restrictions other than the IP address of the encrypting peer.

Command Modes

Crypto map configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

Use the **set identity** command to set the identity to the configured crypto maps. When this command is applied, only the hosts that match a configuration listed within the *name* argument can use that crypto map.

Examples

The following example shows how to configure two IP Security (IPSec) crypto maps and apply the identity to each crypto map. That is, the identity is set to “to-bigbiz” for the first crypto map and “to-little-com” for the second crypto map.

```
! The following is an IPSec crypto map (part of IPSec configuration). It can be used only
! by peers that have been authenticated by DN and if the certificate belongs to BigBiz.
crypto map map-to-bigbiz 10 ipsec-isakmp
 set peer 172.21.114.196
 set transform-set my-transformset
 match address 124
 set identity to-bigbiz
!
crypto identity to-bigbiz
 dn ou=BigBiz
!
!
```

```
! This crypto map can be used only by peers that have been authenticated by hostname
! and if the certificate belongs to little.com.
crypto map map-to-little-com 10 ipsec-isakmp
 set peer 172.21.115.119
 set transform-set my-transformset
 match address 125
 identity to-little-com
!
crypto identity to-little-com
 fqdn little.com
```

Related Commands

Command	Description
crypto identity	Configures the identity of the router with a given list of DNs in the certificate of the router.
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto mib ipsec flowmib history failure size	Associates the identity of the router with the DN in the certificate of the router.
fqdn	Associates the identity of the router with the hostname that the peer used to authenticate itself.

set ip access-group

To check a preencrypted or postdecrypted packet against an access control list (ACL) without having to use the outside physical interface ACL, use the **set ip access-group** command in crypto map configuration mode. To disable the check, use the **no** form of this command.

set ip access-group {*access-list-number* | *access-list-name*} {**in** | **out**}

no set ip access-group {*access-list-number* | *access-list-name*} {**in** | **out**}

Syntax Description

access-list-number	Number of an access list. Values 100 through 199 are used for IP access lists (extended). The values 2000 through 2699 are used for expanded access lists (extended).
access-list-name	Name of an access list.
in	Sets access control for inbound clear-text packets (after decryption).
out	Sets access control for outbound clear-text packets (prior to encryption).

Defaults

No crypto map access ACLs are defined to filter clear-text packets going through the IPSec tunnel.

Command Modes

Crypto map configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The **set ip access-group** command is used after the crypto map has been configured.

Examples

The following example shows that a crypto map access ACL has been configured:

```
Router (config)# crypto map map vpn1 10
Router (config-crypto-map)# set ip access-group 151 in
```

Related Commands

Command	Description
crypto map	Assigns a previously defined crypto map set to an interface so that the interface can provide IPSec services.

set isakmp-profile

To set the Internet Security Association and Key Management Protocol (ISAKMP) profile name, use the **set isakmp-profile** command in crypto map configuration mode. To remove the ISAKMP profile name, use the **no** form of this command.

set isakmp-profile *profile-name*

no set isakmp-profile *profile-name*

Syntax Description

profile-name	Name of the ISAKMP profile.

Defaults

If the ISAKMP profile is not specified in the crypto map entry, the default is to the ISAKMP profile that is on the head. If there is no ISAKMP profile on the head, the default is "none."

Command Modes

Crypto map configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command describes the ISAKMP profile to use when you start the Internet Key Exchange (IKE) exchange.

Before configuring an ISAKMP profile on a crypto map, you should set up the ISAKMP profile.

Examples

The following example shows that an ISAKMP profile has been configured on a crypto map:

```
crypto map vpnmap 10 ipsec-isakmp
 set isakmp-profile vpnprofile
```

Related Commands

Command	Description
crypto ipsec transform-set	Defines a transform set, which is an acceptable combination of security protocols and algorithms.
crypto map (global)	Creates or modifies a crypto map entry.

set nat demux

To enable L2TP—IPSec support for NAT or PAT Windows clients, use the **set nat demux** command in crypto map configuration mode. To disable L2TP—IPSec support, use the **no** form of this command.

set nat demux

no set nat demux

Syntax Description

This command has no arguments or keywords.

Command Default

With this command disabled, Windows clients lose connection when another Windows client establishes an IP Security (IPSec) protected Cisco IOS Layer 2 Tunneling Protocol (L2TP) tunnel to the same Cisco IOS L2TP Network Server (LNS) when there is a network address translation (NAT) or port address translation (PAT) server between the Windows clients and the LNS.

Command Modes

Crypto map configuration

Command History

Release	Modification
12.3(11)T4	This command was introduced.
12.4(1)	This command was integrated into Release 12.4(1).

Usage Guidelines

Use this command if you have an environment with IPSec enabled and consisting of an LNS, and a network address translation (NAT) or port address translation (PAT) server between the Windows clients and the LNS.

This command has been tested only with Windows 2000 L2TP/IPsec clients running hotfix 818043.

You must enter the **crypto map** command if you are using static crypto maps or the **crypto dynamic-map** command if you are using dynamic crypto maps before issuing the **set nat demux** command.

Note If you do not have IPSec enabled, or you do not have a NAT or PAT server, you can have multiple Windows clients connect to a LNS without this command enabled.

Examples

The following example shows how to enable L2TP—IPSec support for NAT or PAT Windows clients for a dynamic crypto map:

```
.
.
.
!Enable virtual private networking.
vpdn enable

! Default L2TP VPDN group
```

```
vpdn-group 1
!
!Enables the LNS to accept dial in requests; specifies L2TP as the tunneling
protocol; specifies the number of the virtual templates used to clone
virtual-access interfaces; specifies an alternate IP address for a VPDN tunnel
accept-dialin.
  protocol l2tp
  virtual-template 1
  source-ip 10.0.0.1
!
!Disables Layer 2 Tunneling Protocol (L2TP) tunnel authentication.
no l2tp tunnel authentication
!
!Defines an Internet Key Exchange (IKE) policy and assigns priority 1.
crypto isakmp policy 1
 encr 3des
 group 2
!
crypto isakmp policy 2
 encr 3des
 authentication pre-share
 group 2
!
!Defines a transform set.
crypto ipsec transform-set vpn esp-3des esp-md5-hmac
 mode transport
crypto mib ipsec flowmib history tunnel size 2
crypto mib ipsec flowmib history failure size 2
!
!Names the dynamic crypto map entry to create (or modify) and enters crypto map
configuration mode.
crypto dynamic-map dyn_map 1
!Specifies which transform sets can be used with the crypto map entry
 set transform-set vpn
!Enables L2TP—IPSec support.
 set nat demux
.
.
.
```

Related Commands

Command	Description
crypto dynamic-map	Names the dynamic crypto map entry to create (or modify) and enters crypto map configuration mode.
crypto map	Names the static crypto map entry to create (or modify) and enters crypto map configuration mode.
show crypto dynamic-map	Displays information about dynamic crypto maps.
show crypto ipsec sa	Displays the settings used by current SAs.
show crypto map	Displays information about static crypto maps.

set peer (IPsec)

To specify an IP Security (IPsec) peer in a crypto map entry, use the **set peer** command in crypto map configuration mode. To remove an IPsec peer from a crypto map entry, use the **no** form of this command.

set peer {*host-name* [**dynamic**] [**default**] | *ip-address* [**default**] }

no set peer {*host-name* [**dynamic**] [**default**] | *ip-address* [**default**] }

Syntax Description

host-name	Specifies the IPsec peer by its hostname. This is the peer's hostname concatenated with its domain name (for example, myhost.example.com).
dynamic	(Optional) The hostname of the IPsec peer will be resolved via a domain name server (DNS) lookup right before the router establishes the IPsec tunnel.
default	(Optional) If there are multiple IPsec peers, designates that the first peer is the default peer.
ip-address	Specifies the IPsec peer by its IP address.

Command Default

No peer is defined.

Command Modes

Crypto map configuration (config-crypto-map)

Command History

Release	Modification
11.2	This command was introduced.
12.3(4)T	The **dynamic** keyword was added.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.3(14)T	The **default** keyword was added.
12.2(33)SRA	The command was integrated into Cisco IOS Release 12.2(33)SRA

Usage Guidelines

Use this command to specify an IPsec peer for a crypto map.

This command is required for all static crypto maps. If you are defining a dynamic crypto map (with the **crypto dynamic-map** command), this command is not required, and in most cases is not used (because, in general, the peer is unknown).

For crypto map entries created with the **crypto map** *map-name seq-num* **ipsec-isakmp** command, you can specify multiple peers by repeating this command. The peer that packets are actually sent to is determined by the last peer that the router heard from (received either traffic or a negotiation request from) for a given data flow. If the attempt fails with the first peer, Internet Key Exchange (IKE) tries the next peer on the crypto map list.

For crypto map entries created with the **crypto map** *map-name seq-num* **ipsec-manual** command, you can specify only one IPsec peer per crypto map. If you want to change the peer, you must first delete the old peer and then specify the new peer.

You can specify the remote IPsec peer by its hostname only if the hostname is mapped to the peer's IP address in a DNS or if you manually map the hostname to the IP address with the **ip host** command.

The dynamic Keyword

When specifying the hostname of a remote IPsec peer via the **set peer** command, you can also issue the **dynamic** keyword, which defers DNS resolution of the hostname until right before the IPsec tunnel has been established. Deferring resolution enables the Cisco IOS software to detect whether the IP address of the remote IPsec peer has changed. Thus, the software can contact the peer at the new IP address.

If the **dynamic** keyword is not issued, the hostname is resolved immediately after it is specified. So, the Cisco IOS software cannot detect an IP address change and, therefore, attempts to connect to the IP address that it previously resolved.

The default Keyword

If there are multiple peers and you specify the **default** keyword, the first peer is designated as the default peer.

If dead peer detection (DPD) detects a failure, the default peer is retried before there is an attempt to connect to the next peer in the peer list.

If the default peer is unresponsive, the next peer in the peer list becomes the new current peer. Future connections through the crypto map will try that peer.

Examples

The following example shows a crypto map configuration when IKE will be used to establish the security associations (SAs). In this example, an SA could be set up to either the IPsec peer at 10.0.0.1 or the peer at 10.0.0.2.

```
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
 set peer 10.0.0.2
```

The following example shows how to configure a router to perform real-time Domain Name System (DNS) resolution with a remote IPsec peer; that is, the hostname of peer is resolved via a DNS lookup right before the router establishes a connection (an IPsec tunnel) with the peer.

```
crypto map secure_b 10 ipsec-isakmp
  match address 140
  set peer b.cisco.com dynamic
  set transform-set xset
interface serial1
  ip address 10.30.0.1
  crypto map secure_b
access-list 140 permit ...
```

The following example shows that the first peer, at IP address 10.1.1.1, is the default peer:

```
crypto map tohub 1 ipsec-isakmp
 set peer 10.1.1.1 default
 set peer 10.2.2.2
```

The following example shows that the peer with the hostname user1 is the default peer.

```
crypto map tohub 2 ipsec-isakmp
 set peer user1 dynamic default
 set peer user2 dynamic
```

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPsec traffic.
match address (IPSec)	Specifies an extended access list for a crypto map entry.
set pfs	Specifies that IPsec should ask for PFS when requesting new SAs for this crypto map entry, or that IPsec requires PFS when receiving requests for new SAs.
set security-association level per-host	Specifies that separate IPsec SAs should be requested for each source/destination host pair.
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPsec SAs.
set session-key	Specifies the IPsec session keys within a crypto map entry.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPSec)	Displays the crypto map configuration.

set pfs

To optionally specify that IP security (IPsec) requests the perfect forward secrecy (PFS) Diffie-Hellman (DH) prime modulus group identifier when requesting new security associations (SAs) for a crypto map entry or when IPsec requires PFS when receiving requests for new SAs, use the **set pfs** command in crypto map configuration mode. To specify that IPsec should not request PFS during the DH exchange, use the **no** form of this command.

set pfs {**group1 | group2 | group5 | group14 | group15 | group16 | group19 | group20**}

no set pfs

Syntax Description

group1	Specifies the 768-bit DH identifier.
group2	Specifies the 1024-bit DH identifier.
group5	Specifies the 1536-bit DH identifier.
group14	Specifies the 2048-bit DH identifier.
group15	Specifies the 3072-bit DH identifier.
group16	Specifies the 4096-bit DH identifier.
group19	Specifies the 256-bit elliptic curve DH (ECDH) identifier.
group20	Specifies the 384-bit ECDH identifier.

Defaults

By default, PFS is not requested. If no group is specified with this command, the **group1** keyword is used as the default.

Command Modes

Crypto map configuration (config-crypto-map)

Command History

Release	Modification
11.3 T	This command was introduced.
12.1(1.3)T	Support was added for DH group 5.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	Support for IPv6 was added.
Cisco IOS XE Release 2.2	Support was added for DH groups 14, 15, and 16 on the Cisco ASR 1000 series routers.
12.4(22)T	Support for DH groups 14, 15, and 16 on the Cisco ASR 1000 series routers was integrated into Cisco IOS Release 12.4(22)T.
15.1(2)T	This command was modified. DH groups 19 and 20 were added in Cisco IOS Release 15.1(2)T.

Usage Guidelines

This command is available for **ipsec-isakmp** crypto map entries and dynamic crypto map entries for both IKEv1 and IKEv2.

During negotiation, this command causes IPsec to request PFS when requesting new security associations for the crypto map entry. The default (**group1**) is sent if the **set pfs** statement does not specify a group. If the peer initiates the negotiation and the local configuration specifies PFS, the remote peer must perform a PFS exchange or the negotiation will fail. If the local configuration does not specify a group, a default of **group1** will be assumed, and an offer of either **group1** or **group2** will be accepted. If the local configuration specifies **group2**, that group *must* be part of the offer of the peer or the negotiation will fail. If the local configuration does not specify PFS, it will accept any offer of PFS from the peer.

PFS adds another level of security; if one key is ever cracked by an attacker, then only the data sent with that key will be compromised. Without PFS, data sent with other keys could be compromised also.

With PFS, every time a new security association is negotiated, a new DH exchange occurs. (This exchange requires additional processing time.)

The 1024-bit DH prime modulus group, **group2**, provides more security than **group1** but requires more processing time than **group1**.

The group chosen must be strong enough (have enough bits) to protect the IPsec keys during negotiation. While there is some disagreement regarding how many bits are necessary in the DH group to protect a specific key size, it is generally agreed that **group14** is good protection for 128-bit keys, **group15** is good protection for 192-bit keys, and **group16** is good protection for 256-bit keys.

Note **group5** may be used for 128-bit keys, but **group14** is better.

The ISAKMP group and the IPsec PFS group should be the same if PFS is used. If PFS is not used, a group is not configured in the IPsec crypto map.

Examples

The following example specifies that PFS should be used whenever a new security association is negotiated for the crypto map mymap 10:

```
crypto map mymap 10 ipsec-isakmp
 set pfs group2
```

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
crypto map (global IPsec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map (interface IPsec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPsec traffic.
match address (IPsec)	Specifies an extended access list for a crypto map entry.
set peer (IPsec)	Specifies an IPsec peer in a crypto map entry.

Command	Description
set security-association level per-host	Specifies that separate IPsec security associations should be requested for each source/destination host pair.
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPsec security associations.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPsec)	Displays the crypto map configuration.

set reverse-route

To define a distance metric for each static route or to tag a reverse route injection (RRI)-created route, use the **set reverse-route** command in crypto map configuration or IPsec profile configuration mode. To delete the tag or distance metric, use the **no** form of the command.

set reverse-route [**distance** *number* | **tag** *tag-id* | **gateway** *next-hop*]

no set reverse-route [**distance** *number* | **tag** *tag-id* | **gateway**]

Syntax Description

distance *number*	(Optional) Defines a distance metric for each static route. The range is from 1 to 255.
tag *tag-id*	(Optional) Creates a route and tags it. The tag value can be used as a match value for controlling redistribution using route maps.
gateway *next-hop*	(Optional) Defines the next hop IP address of the preferred gateway through which encrypted traffic can be routed.

Command Default

The distance metric is 1 and the tag is 0.

Command Modes

Crypto map configuration (config-crypto-map)
IPsec profile configuration (config-crypto-profile)

Command History

Release	Modification
12.4(15)T	This command was introduced. This command replaces the **reverse-route tag** command.
Cisco IOS XE Release 3.2S	This command was modified. The **gateway** keyword and *next-hop* argument were added.

Usage Guidelines

This command can be applied on a per-crypto map basis or to a virtual tunnel interface (VTI) in a reverse route injection configuration.

RRI provides a scalable mechanism to dynamically learn and advertise the IP address and subnets, which belong to a remote site that connects through an IP Security (IPsec) Virtual Private Network (VPN) tunnel.

When enabled in an IPsec crypto map, RRI learns all the subnets from any network that is defined in the crypto access control list (ACL) as the destination network. The learned routes are installed into the local routing table as static routes that point to the encrypted interface. When the IPsec tunnel is torn down, the associated static routes are removed. These static routes may then be redistributed into other dynamic routing protocols so that they can be advertised to other parts of the network (usually by redistributing RRI routes into dynamic routing protocols on the core side).

The **set reverse-route** command provides a way to configure a server so that a dynamically learned route can take precedence over static routes. The static routes are used only in the absence of the dynamically learned route.

Inserting an RRI in the remote peer through a gateway that is configured in the crypto IPsec profile ensures that the traffic to the remote peer is always routed through the configured gateway.

If you configure the RRI gateway when there are no sessions, then no changes occur. A route to the remote peer is added only when a new security association (SA) becomes active.

To change to a new gateway when there are active sessions, you must delete the active sessions. You cannot add, delete, or change a gateway configuration when there are active sessions.

The gateway configuration scenarios with respect to sessions are exhibited irrespective of whether Front Virtual Routing and Forwarding (FVRF) has been configured or not.

Examples

The following example shows how to set the value of the metric distance for each dynamic route to 20 in a crypto map situation. The configuration is on an Easy VPN server.

```
crypto dynamic-map mode 1
 set security-association lifetime seconds 300
 set transform-set 3dessha
 set isakmp-profile profile2
 set reverse-route distance 20
 reverse-route
```

The following example shows how to set the value of the metric distance for each dynamic route to 20 for a virtual tunnel interface (VTI). The configuration is on an Easy VPN server.

```
crypto isakmp profile profile1
 keyring mykeyring
 match identity group examplegroup
 client authentication list authenlist
 isakmp authorization list autholist
 client configuration address respond
 virtual-template 1
crypto ipsec profile vi
 set transform-set 3dessha
 set reverse-route distance 20
 set reverse-route gateway 10.0.0.1
 set isakmp-profile profile1
!
interface Virtual-Template1 type tunnel
 ip unnumbered
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vi
```

Related Commands

Command	Description
debug crypto ipsec	Displays IPsec events.
reverse-route	Creates source proxy information for a crypto map entry.

set security-association idle-time

To specify the maximum amount of time for which the current peer can be idle before the default peer is used, use the **set security-association idle-time** command in crypto map configuration mode. To disable this feature, use the **no** form of this command.

set security-association idle-time *seconds* [**default**]

no set security-association idle-time *seconds* [**default**]

Syntax Description

seconds	Number of seconds for which the current peer can be idle before the default peer is used. Although the command will accept values for *seconds* ranging from 60 to 86400 seconds, the configured value will be rounded up to the next multiple of 600 seconds (ten minutes).
default	(Optional) Specifies that the next connection is directed to the default peer. Default: If the **default** keyword is not specified and there is a connection timeout, the current peer remains unchanged.

Command Default

The default peer is not used if the current peer times out.

Command Modes

Crypto map configuration (config-crypto-map)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRA	The command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command is optional. Use this command if you want the default peer to be used if the current peer times out. If there is a timeout to the current peer, the connection to that peer is closed. The next time a connection is initiated, it is directed to the default peer specified in the **set peer** command.

The configured value for *seconds* is rounded up to the next multiple of 600 seconds (ten minutes), and the rounded value becomes the polling interval for peer idle detection. Because the idle condition must be observed in two successive pollings, the period of inactivity may last up to twice the polling period before the connection to the idle peer can be closed.

Examples

In the following example, if the current peer is idle for at least 750 seconds, the default peer 10.1.1.1 (which was specified in the **set peer** command) is used for the next attempted connection:

```
crypto map tohub 1 ipsec-isakmp
 set peer 10.1.1.1 default
 set peer 10.2.2.2
 set security-association idle-time 750 default
```

In this example, the configured value of 750 seconds will be rounded up to 1200 seconds (the next multiple of 600), which becomes the idle polling interval. The connection to the idle peer will be closed after two successive idle pollings, resulting in an inactivity period of between 1200 and 2400 seconds before the connection is closed.

Related Commands

Command	Description
set peer (IPSec)	Specifies an IPsec peer in a crypto map entry.

set security-association level per-host

To specify that separate IP Security security associations should be requested for each source/destination host pair, use the **set security-association level per-host** command in crypto map configuration mode. To specify that one security association should be requested for each crypto map access list **permit** entry, use the **no** form of this command.

set security-association level per-host

no set security-association level per-host

Syntax Description

This command has no arguments or keywords.

Defaults

For a given crypto map, all traffic between two IPSec peers matching a single crypto map access list **permit** entry will share the same security association.

Command Modes

Crypto map configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is only available for **ipsec-isakmp** crypto map entries and is not supported for dynamic crypto map entries.

When you use this command, you need to specify that a separate security association should be used for each source/destination host pair.

Normally, within a given crypto map, IPSec will attempt to request security associations at the granularity specified by the access list entry. For example, if the access list entry permits IP protocol traffic between subnet A and subnet B, IPSec will attempt to request security associations between subnet A and subnet B (for any IP protocol), and unless finer-grained security associations are established (by a peer request), all IPSec-protected traffic between these two subnets would use the same security association.

This command causes IPSec to request separate security associations for each source/destination host pair. In this case, each host pairing (where one host was in subnet A and the other host was in subnet B) would cause IPSec to request a separate security association.

With this command, one security association would be requested to protect traffic between host A and host B, and a different security association would be requested to protect traffic between host A and host C.

The access list entry can specify local and remote subnets, or it can specify a host-and-subnet combination. If the access list entry specifies protocols and ports, these values are applied when establishing the unique security associations.

Use this command with care, as multiple streams between given subnets can rapidly consume system resources.

Examples

The following example shows what happens with an access list entry of **permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255** and a per-host level:

- A packet from 10.1.1.1 to 10.2.2.1 will initiate a security association request, which would look like it originated via **permit ip host 10.1.1.1 host 10.2.2.1**.
- A packet from 10.1.1.1 to 10.2.2.2 will initiate a security association request, which would look like it originated via **permit ip host 10.1.1.1 host 10.2.2.2**.
- A packet from 10.1.1.2 to 10.2.2.1 will initiate a security association request, which would look like it originated via **permit ip host 10.1.1.2 host 10.2.2.1**.

Without the per-host level, any of the above packets will initiate a single security association request originated via **permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255**.

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
match address (IPSec)	Specifies an extended access list for a crypto map entry.
set peer (IPSec)	Specifies an IPSec peer in a crypto map entry.
set pfs	Specifies that IPSec should ask for PFS when requesting new security associations for this crypto map entry, or that IPSec requires PFS when receiving requests for new security associations.
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPSec security associations.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPSec)	Displays the crypto map configuration.

set security-association lifetime

To override (for a particular crypto map entry) the global lifetime value, which is used when negotiating IP Security security associations, use the **set security-association lifetime** command in crypto map configuration mode. To reset a crypto map entry's lifetime value to the global value, use the **no** form of this command.

set security-association lifetime {**seconds** *seconds* | **kilobytes** *kilobytes* | **kilobytes disable**}

no set security-association lifetime {**seconds** | **kilobytes** | **kilobytes disable**}

Syntax Description

seconds *seconds*	Specifies the number of seconds a security association will live before expiring.
kilobytes *kilobytes*	Specifies the volume of traffic (in kilobytes) that can pass between IPsec peers using a given security association before that security association expires.
kilobytes disable	Disables the IPsec security association (SA) rekey based on the traffic-volume lifetime (in kilobytes). If the **no** form is used with these keywords, lifetime settings return to the default settings.

Defaults

The crypto map's security associations are negotiated according to the global lifetimes.

Command Modes

Crypto map configuration (config-crypto-map)

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	Support for IPv6 was added.
12.2(33)SXI	The **disable** keyword was added. **Note** This keyword addition is for only Cisco IOS Release 12.2(33)SXI.
15.0(1)M	The **disable** keyword was added.

Usage Guidelines

This command is available only for **ipsec-isakmp** crypto map entries and dynamic crypto map entries.

IPsec security associations use shared secret keys. These keys and their security associations time out together.

Assuming that the particular crypto map entry has lifetime values configured, when the router requests new security associations during security association negotiation, it will specify its crypto map lifetime value in the request to the peer; it will use this value as the lifetime of the new security associations.

When the router receives a negotiation request from the peer, it will use the smaller of the lifetime value proposed by the peer or the locally configured lifetime value as the lifetime of the new security associations.

There are two lifetimes: a "timed" lifetime and a "traffic-volume" lifetime. The session keys or security association expires after the first of these lifetimes is reached.

Note IPsec SA rekey can be triggered either by a timed lifetime or by a traffic-volume lifetime. To control rekey, it is recommended that you use the timed lifetime rather than the traffic-volume lifetime. When a small traffic-volume lifetime is used for IPsec SA, it causes frequent IPsec SA rekeys. High throughput of encryption or decryption traffic can cause intermittent packet drops. The minimum traffic-volume lifetime threshold of 2560 kilobytes is *not* recommended on IPsec SAs that protect a medium-to-high throughput data link because this setting can cause packet drops during rekey.

If you change a lifetime, the change will not be applied to existing security associations, but will be used in subsequent negotiations to establish security associations for data flows supported by this crypto map entry. If you want the new settings to take effect sooner, you can clear all or part of the security association database by using the **clear crypto sa** command. Refer to the **clear crypto sa** command for more detail.

To change the timed lifetime, use the **set security-association lifetime seconds** form of the command. The timed lifetime causes the keys and security association to time out after the specified number of seconds have passed.

To change the traffic-volume lifetime, use the **set security-association lifetime kilobytes** form of the command. The traffic-volume lifetime causes the key and security association to time out after the specified amount of traffic (in kilobytes) has been protected by the security association's key.

Shorter lifetimes can make it harder to mount a successful key recovery attack, because the attacker has less data encrypted under the same key to work with. However, shorter lifetimes need more CPU processing time.

The lifetime values are ignored for manually established security associations (security associations installed via an **ipsec-manual** crypto map entry).

How The Lifetimes Work

Assuming that the particular crypto map entry does not have lifetime values configured, when the router requests new security associations it will specify its global lifetime values in the request to the peer; it will use this value as the lifetime of the new security associations. When the router receives a negotiation request from the peer, it will use the smaller of either the lifetime value proposed by the peer or the locally configured lifetime value as the lifetime of the new security associations.

The security association (and corresponding keys) will expire according to whichever occurs sooner, either after the **seconds** time out or after the **kilobytes** amount of traffic is passed.

A new security association is negotiated *before* the lifetime threshold of the existing security association is reached, to ensure that a new security association is ready for use when the old one expires. The **seconds** lifetime and the **kilobytes** lifetime each have a jitter mechanism to avoid security association rekey collisions. The new security association is negotiated either (30 plus a random number of) seconds before the **seconds** lifetime expires or when the traffic volume reaches (90 minus a random number of) percent of the **kilobytes** lifetime (whichever occurs first).

If no traffic has passed through the tunnel during the entire life of the security association, a new security association is not negotiated when the lifetime expires. Instead, a new security association will be negotiated only when IPsec sees another packet that should be protected.

Disabling the Traffic-Volume Lifetime

The **set security-association lifetime kilobytes disable** form of the command disables the traffic-volume lifetime. Disabling the traffic-volume lifetime affects only the router on which IPsec SA rekey based on traffic-volume lifetime is configured. It does not affect the peer router's behavior or the current router's IPsec SA time-based (seconds) rekey. The **set security-association lifetime kilobytes disable** form of the command is useful when the IPsec SAs are protecting a high bandwidth data link (10-gigabit Ethernet). This option can be used to reduce packet loss in high traffic environments and to prevent frequent rekeys that are triggered by reaching the volume lifetimes.

Note The traffic-volume lifetime can also be disabled by entering the **crypto ipsec security-association lifetime kilobytes disable** command.

Examples

The following example shortens the timed lifetime for a particular crypto map entry, because there is a higher risk that the keys could be compromised for security associations belonging to the crypto map entry. The traffic-volume lifetime is not changed because there is not a high volume of traffic anticipated for these security associations. The timed lifetime is shortened to 2700 seconds (45 minutes).

```
crypto map mymap 10 ipsec-isakmp
 set security-association lifetime seconds 2700
```

The following example shows that the **kilobytes disable** keyword has been used to disable the volume lifetime.

```
set security-association lifetime kilobytes disable
```

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
crypto ipsec security-association lifetime	Changes global lifetime values used when negotiating IPsec security associations.
crypto map (global IPsec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map (interface IPsec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPsec traffic.
match address (IPsec)	Specifies an extended access list for a crypto map entry.
set peer (IPsec)	Specifies an IPsec peer in a crypto map entry.
set pfs	Specifies that IPsec should ask for PFS when requesting new security associations for this crypto map entry, or that IPsec requires PFS when receiving requests for new security associations.
set security-association level per-host	Specifies that separate IPsec security associations should be requested for each source/destination host pair.

Command	Description
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPsec)	Displays the crypto map configuration.

set security-association replay disable

To disable anti-replay checking for a particular crypto map, dynamic crypto map, or crypto profile, use the **set security-association replay disable** command in crypto map configuration or crypto profile configuration mode. To enable anti-replay checking, use the **no** form of this command.

set security-association replay disable

no set security-association replay disable

Syntax Description

This command has no arguments or keywords.

Defaults

Anti-replay checking is enabled.

Command Modes

Crypto map configuration
Crypto profile configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF6	This command was integrated into Cisco IOS Release 12.2(18)SXF6.

Examples

The following example shows that anti-replay checking has been disabled for the crypto map named "mymap."

```
crypto map mymap 30
set security-association replay disable
```

Related Commands

Command	Description
set security-association replay window-size	Controls the SAs that are created using the policy specified by a particular crypto map, dynamic crypto map, or crypto profile.

set security-association replay window-size

To control the security associations (SAs) that are created using the policy specified by a particular crypto map, dynamic crypto map, or crypto profile, use the **set security-association replay window-size** command in crypto map configuration or crypto profile configuration mode. To reset the crypto map to follow the global configuration that was specified by the **crypto ipsec security-association replay window-size** command, use the **no** form of this command.

set security-association replay window-size [*N*]

no set security-association replay window-size

Syntax Description

N	(Optional) Size of the window. The value can be 64, 128, 256, 512, or 1024. This value sets the window size for a particular crypto map, dynamic crypto map, or crypto profile.

Defaults

Window size is not set.

Command Modes

Crypto map configuration
Crypto profile configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF6	This command was integrated into Cisco IOS Release 12.2(18)SXF6.

Examples

The following example shows that the SA window size has been set to 256 for the crypto map named "mymap":

```
crypto map mymap 10
set security-association replay window-size 256
```

Related Commands

Command	Description
set security-association replay disable	Disables anti-replay checking for a particular crypto map, dynamic crypto map, or crypto profile.

set security-policy limit

To define an upper limit to the number of flows that can be created for an individual virtual access interface, use the **set security-policy limit** command in IPsec profile configuration mode. To remove the limitation, use the **no** form of the command.

set security-policy limit *maximum-limit*

no set security-policy limit

Syntax Description

maximum-limit	The number of security policy entries that can be negotiated with the peer. The range is from 0 to 50000.

Command Default

The upper limit to the number of flows that can be created for an individual virtual access interface is not defined.

Command Modes

IPsec profile configuration (config-crypto-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

The **set security-policy limit** command is disabled by default. If the maximum limit is changed, this change is applied to the existing session. If the maximum limit is set to 0, then no new IPsec security associations (SAs) are created.

Examples

The following example shows how to limit the number of flows that can be created for an individual virtual access interface to 5.

```
crypto ipsec profile ipsec-profile-1
 set security-policy limit 5
```

Related Commands

Command	Description
crypto ipsec profile	Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec routers and to enter IPsec profile configuration mode.
crypto isakmp profile	Defines an ISAKMP profile and IPsec user sessions.
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically when virtual access interfaces are created.

set session-key

To manually specify the IP Security session keys within a crypto map entry, use the **set session-key** command in crypto map configuration mode. This command is available only for **ipsec-manual** crypto map entries. To remove IPSec session keys from a crypto map entry, use the **no** form of this command.

Authentication Header (AH) Protocol Syntax

set session-key {**inbound** | **outbound**} **ah** *spi hex-key-string*

no set session-key {**inbound** | **outbound**} **ah**

Encapsulation Security Protocol (ESP) Syntax

set session-key {**inbound** | **outbound**} **esp** *spi cipher hex-key-string* [**authenticator** *hex-key-string*]

no set session-key {**inbound** | **outbound**} **esp**

Syntax Description

inbound	Sets the inbound IPSec session key. (You must set both inbound and outbound keys.)
outbound	Sets the outbound IPSec session key. (You must set both inbound and outbound keys.)
ah	Sets the IPSec session key for the AH protocol. Use when the crypto map entry's transform set includes an AH transform.
esp	Sets the IPSec session key for ESP. Use when the crypto map entry's transform set includes an ESP transform.
spi	Specifies the security parameter index (SPI), a number that is used to uniquely identify a security association. The SPI is an arbitrary number you assign in the range of 256 to 4,294,967,295 (FFFF FFFF). You can assign the same SPI to both directions and both protocols. However, not all peers have the same flexibility in SPI assignment. For a given destination address/protocol combination, unique SPI values must be used. The destination address is that of the router if inbound, the peer if outbound.
hex-key-string	Specifies the session key; enter in hexadecimal format. This is an arbitrary hexadecimal string of 8, 16, or 20 bytes. If the crypto map's transform set includes a DES algorithm, specify at least 8 bytes per key. If the crypto map's transform set includes an MD5 algorithm, specify at least 16 bytes per key. If the crypto map's transform set includes an SHA algorithm, specify 20 bytes per key. Keys longer than the above sizes are simply truncated.
cipher	Indicates that the key string is to be used with the ESP encryption transform.
authenticator	(Optional) Indicates that the key string is to be used with the ESP authentication transform. This argument is required only when the crypto map entry's transform set includes an ESP authentication transform.

Defaults

No session keys are defined by default.

Command Modes

Crypto map configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to define IPSec keys for security associations via **ipsec-manual** crypto map entries. (In the case of **ipsec-isakmp** crypto map entries, the security associations with their corresponding keys are automatically established via the IKE negotiation.)

If the crypto map's transform set includes an AH protocol, you must define IPSec keys for AH for both inbound and outbound traffic. If the crypto map's transform set includes an ESP encryption protocol, you must define IPSec keys for ESP encryption for both inbound and outbound traffic. If your transform set includes an ESP authentication protocol, you must define IPSec keys for ESP authentication for inbound and outbound traffic.

When you define multiple IPSec session keys within a single crypto map, you can assign the same security parameter index (SPI) number to all the keys. The SPI is used to identify the security association used with the crypto map. However, not all peers have the same flexibility in SPI assignment. You should coordinate SPI assignment with your peer's operator, making certain that the same SPI is not used more than once for the same destination address/protocol combination.

Security associations established via this command do not expire (unlike security associations established via IKE).

Session keys at one peer must match the session keys at the remote peer.

If you change a session key, the security association using the key will be deleted and reinitialized.

Examples

The following example shows a crypto map entry for manually established security associations. The transform set "t_set" includes only an AH protocol.

```
crypto ipsec transform-set t_set ah-sha-hmac

crypto map mymap 20 ipsec-manual
 match address 102
 set transform-set t_set
 set peer 10.0.0.21
 set session-key inbound ah 300 11111111111111111111111111111111111111111
 set session-key outbound ah 300 22222222222222222222222222222222222222222
```

The following example shows a crypto map entry for manually established security associations. The transform set "someset" includes both an AH and an ESP protocol, so session keys are configured for both AH and ESP for both inbound and outbound traffic. The transform set includes both encryption and authentication ESP transforms, so session keys are created for both using the **cipher** and **authenticator** keywords.

```
crypto ipsec transform-set someset ah-sha-hmac esp-des esp-sha-hmac

crypto map mymap 10 ipsec-manual
 match address 101
 set transform-set someset
 set peer 10.0.0.1
 set session-key inbound ah 300 9876543210987654321098765432109876543210
 set session-key outbound ah 300 fedcbafedcbafedcbafedcbafedcbafedcbafedc
 set session-key inbound esp 300 cipher 0123456789012345
  authenticator 00001111222233334444555566667777788889999
 set session-key outbound esp 300 cipher abcdefabcdefabcd
  authenticator 99998888777766665555444433332222111110000
```

Related Commands

Command	Description
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
match address (IPSec)	Specifies an extended access list for a crypto map entry.
set peer (IPSec)	Specifies an IPSec peer in a crypto map entry.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPSec)	Displays the crypto map configuration.

set transform-set

To specify which transform sets can be used with the crypto map entry, use the **set transform-set** command in crypto map configuration mode. To remove all transform sets from a crypto map entry, use the **no** form of this command.

set transform-set *transform-set-name* [*transform-set-name2...transform-set-name6*]

no set transform-set

Syntax Description

transform-set-name	Name of the transform set. For an **ipsec-manual** crypto map entry, you can specify only one transform set. For an **ipsec-isakmp** or dynamic crypto map entry, you can specify up to six transform sets.

Command Default

No transform sets are included by default.

Command Modes

Crypto map configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.4(4)T	Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is required for all static and dynamic crypto map entries.

Use this command to specify which transform sets to include in a crypto map entry.

For an **ipsec-isakmp** crypto map entry, you can list multiple transform sets with this command. List the higher priority transform sets first.

If the local router initiates the negotiation, the transform sets are presented to the peer in the order specified in the crypto map entry. If the peer initiates the negotiation, the local router accepts the first transform set that matches one of the transform sets specified in the crypto map entry.

The first matching transform set that is found at both peers is used for the security association. If no match is found, IPSec will not establish a security association. The traffic will be dropped because there is no security association to protect the traffic.

For an **ipsec-manual** crypto map entry, you can specify only one transform set. If the transform set does not match the transform set at the remote peer's crypto map, the two peers will fail to correctly communicate because the peers are using different rules to process the traffic.

If you want to change the list of transform sets, re-specify the new list of transform sets to replace the old list. This change is only applied to crypto map entries that reference this transform set. The change will not be applied to existing security associations, but will be used in subsequent negotiations to establish new security associations. If you want the new settings to take effect sooner, you can clear all or part of the security association database by using the **clear crypto sa** command.

Any transform sets included in a crypto map must previously have been defined using the **crypto ipsec transform-set** command.

Examples

The following example defines two transform sets and specifies that they can both be used within a crypto map entry. (This example applies only when IKE is used to establish security associations. With crypto maps used for manually established security associations, only one transform set can be included in a given crypto map entry.)

```
crypto ipsec transform-set my_t_set1 esp-des esp-sha-hmac
crypto ipsec transform-set my_t_set2 ah-sha-hmac esp-des esp-sha-hmac

crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1 my_t_set2
 set peer 10.0.0.1
 set peer 10.0.0.2
```

In this example, when traffic matches access list 101, the security association can use either transform set “my_t_set1” (first priority) or “my_t_set2” (second priority) depending on which transform set matches the remote peer’s transform sets.

sgbp aaa authentication

To enable a Stack Group Bidding Protocol (SGBP) authentication list, use the **sgbp aaa authentication** command in global configuration mode. To disable the SGBP authentication list, use the **no** form of this command.

sgbp aaa authentication list *list-name*

no sgbp aaa authentication list *list-name*

Syntax Description

list *list-name*	Name of a list of methods of authentication to use.

Defaults

A SGBP authentication list is not enabled. You must use the same authentication, authorization and accounting (AAA) method list as PPP usersl.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command introduced.

Usage Guidelines

Use the **sgbp aaa authentication** command to create a list different from the AAA list that is used by PPP users.

Examples

The following example shows how to create the AAA list "SGBP" that is to be used by SGBP users:

```
Router(config)# sgbp aaa authentication list SGBP
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP.
aaa authentication sgbp	Specifies one or more AAA authentication methods for SGBP.
ppp authentication	Enables at least one PPP authentication protocol and to specifies the order in which the protocols are selected on the interface.

show aaa attributes

To display the mapping between an authentication, authorization, and accounting (AAA) attribute number and the corresponding AAA attribute name, use the **show aaa attributes** command in EXEC configuration mode.

show aaa attributes [**protocol radius**]

Syntax Description

protocol radius	(Optional) Displays the mapping between a RADIUS attribute and a AAA attribute name and number.

Command Modes

EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	The **protocol radius** keyword was added.
12.3(14)T	T.38 fax relay call statistics were made available to Call Detail Records (CDRs) through Vendor-Specific Attributes (VSAs) and added to the call log.

Examples

The following example is sample output for the **show aaa attributes** command. In this example, all RADIUS attributes that have been enabled are displayed.

```
Router# show aaa attributes protocol radius

AAA ATTRIBUTE LIST:
    Type=1     Name=disc-cause-ext                Format=Enum
        Protocol:RADIUS
        Non-Standard  Type=195   Name=Ascend-Disconnect-Cau Format=Enum
        Cisco VSA     Type=1     Name=Cisco AVpair          Format=String
    Type=2     Name=Acct-Status-Type              Format=Enum
        Protocol:RADIUS
        IETF          Type=40    Name=Acct-Status-Type      Format=Enum
    Type=3     Name=acl                           Format=Ulong
        Protocol:RADIUS
        IETF          Type=11    Name=Filter-Id             Format=Binary
    Type=4     Name=addr                          Format=IPv4 Address
        Protocol:RADIUS
        IETF          Type=8     Name=Framed-IP-Address     Format=IPv4 Addre
    Type=5     Name=addr-pool                     Format=String
        Protocol:RADIUS
        Non-Standard  Type=218   Name=Ascend-IP-Pool        Format=Ulong
    Type=6     Name=asyncmap                      Format=Ulong
        Protocol:RADIUS
        Non-Standard  Type=212   Name=Ascend-Asyncmap       Format=Ulong
    Type=7     Name=Authentic                     Format=Enum
        Protocol:RADIUS
        IETF          Type=45    Name=Authentic             Format=Enum
    Type=8     Name=autocmd                       Format=String
```

The following example is sample output for the **show aaa attributes** command. In this example, all the T.38 fax relay statistics are displayed.

```
Router# show aaa attributes
!
    Type=485   Name=originating-line-info          Format=Ulong
    Type=486   Name=charge-number                  Format=String
    Type=487   Name=transmission-medium-req        Format=Ulong
    Type=488   Name=redirecting-number             Format=String
    Type=489   Name=backward-call-indicators       Format=String
    Type=490   Name=remote-media-udp-port          Format=Ulong
    Type=491   Name=remote-media-id                Format=String
    Type=492   Name=supp-svc-xfer-by               Format=String
    Type=493   Name=faxrelay-start-time            Format=String
    Type=494   Name=faxrelay-max-jit-buf-depth     Format=String
    Type=495   Name=faxrelay-jit-buf-ovflow        Format=String
    Type=496   Name=faxrelay-mr-hs-mod             Format=String
    Type=497   Name=faxrelay-init-hs-mod           Format=String
    Type=498   Name=faxrelay-num-pages             Format=String
    Type=499   Name=faxrelay-direction             Format=String
    Type=500   Name=faxrelay-ecm-in-use            Format=String
    Type=501   Name=faxrelay-encap-prot            Format=String
    Type=502   Name=faxrelay-nsf-country-code      Format=String
    Type=503   Name=faxrelay-nsf-manuf-code        Format=String
    Type=504   Name=faxrelay-fax-success           Format=String
    Type=505   Name=faxrelay-tx-packets            Format=String
    Type=506   Name=faxrelay-rx-packets            Format=String
```

Table 62 provides an alphabetical listing of the fields displayed in the output of the **show aaa attributes** command displaying T.38 statistics and a description of each field.

Table 62 show aaa attributes Field Descriptions

Field	Description
Format=Ulong	Format type is ULong.
Format=String	Format type is string.
Name=backward-call-indicators	Backward call indicator.
Name=charge-number	Charge number.
Name=faxrelay-direction	Direction of fax relay.
Name=faxrelay-ecm-in-use	Error correction mode in use for the fax relay.
Name=faxrelay-encap-prot	Encapsulation protocol for fax relay.
Name=faxrelay-fax-success	Fax relay success.
Name=faxrelay-init-hs-mod	Fax relay initial high-speed modulation.
Name=faxrelay-jit-buf-ovflow	Fax relay jitter buffer overflow.
Name=faxrelay-max-jit-buf-depth	Fax relay maximum jitter buffer depth.
Name=faxrelay-mr-hs-mod	Fax relay most recent high speed modulation.
Name=faxrelay-num-pages	Fax relay number of fax pages.
Name=faxrelay-nsf-country-code	Fax relay Nonstandard Facilities (NSF) country code.
Name=faxrelay-nsf-manuf-code	Fax relay NSF manufacturers code.
Name=faxrelay-rx-packets	Fax relay received packets
Name=faxrelay-start-time	Fax relay start time.

Table 62 show aaa attributes Field Descriptions (continued)

Field	Description
Name=faxrelay-tx-packets	Fax relay transmitted packets.
Name=originating-line-info	Originating line information.
Name=redirecting-number	Redirecting number.
Name=remote-media-id	Remote media ID.
Name=remote-media-udp-port	Remote media UDP port.
Name=supp-svc-xfer-by	Supplementary service transfer.
Name=transmission-medium-req	Transmission medium requirement.
Type=	Type of fax relay string.

Related Commands

Command	Description
debug voip aaa	Enables debugging messages for gateway authentication, authorization, and accounting (AAA) to be sent to the system console.

show aaa cache filterserver

To display the cache status, use the **show aaa cache filterserver** command in user EXEC or privileged EXEC mode.

show aaa cache filterserver {**acl** | **pending**}

Syntax Description

acl	Shows the contents of the access control cache at the last refresh.
pending	Shows the contents of the pending call cache, which references filters that have not received a response from the RADIUS server.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4T	The **acl** and **pending** keywords were added.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The **show aaa cache filterserver** command shows how many times a particular filter has been referenced or refreshed. This function may be used in administration to determine which filters are actually being used.

Examples

The following is sample output for the **show aaa cache filterserver** command using the **acl** and **pending** keywords:

```
Router# show aaa cache filterserver acl

Filter     Server          Age Expires Refresh Access-Control-Lists
-------------------------------------------------------------------------------
aol        10.2.3.4          0    1440     100 ip in icmp drop
                                               ip out icmp drop
                                               ip out forward tcp dstip 10.2.3.4
msn        10.2.3.4         N/A   Never       2 ip in tcp drop
msn2       10.2.3.4         N/A   Never       2 ip in tcp drop
vone       10.2.3.4         N/A   Never       0 ip in tcp drop
```

The following is sample output for the **show aaa cache filterserver** command using the **pending** keyword:

```
Router# show aaa cache filterserver pending

AAA pending cache:
Filter Age Expires Refresh
-------------------------------------------------------------------------------
myfilter N/A Never N/A call 0x501802D8 (00000085)
```

Table 63 describes the significant fields shown in the display.

Table 63 show aaa cache filterserver Field Descriptions

Field	Description
Filter	Filter name
Server	RADIUS server IP address
Age	When to expire a cache entry (in minutes)
Expires	Number of minutes in which a cache entry will expire
Refresh	Number of times a cache has been refreshed
Access-Control-Lists	Access control list (ACL) of the server

Related Commands

Command	Description
aaa authorization cache filterserver	Enables AAA authorization caches and the downloading of ACL configurations from a RADIUS filter server.

show aaa cache group

To display all the cache entries stored by the authentication, authorization, and accounting (AAA) cache, use the **show aaa cache group** command in privileged EXEC mode.

show aaa cache group *name* {**all** | **profile** *name*}

Syntax Description

name	Text string representing a cache server group.
all	Displays all server group profile details.
profile *name*	Displays the specified individual server group profile details.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Usage Guidelines

Use the **show aaa cache group** command to display all cache entries for a specific group.

Examples

The following example shows how to display all cache entries for a group. The fields are self-explanatory.

```
Router# show aaa cache group sg1

-----------------------------------------------------------
 Entries in Profile dB SG1 for exact match
-----------------------------------------------------------
Profile: .*user*
Updated: 00:00:33
Parse User: Y
Authen User: Y
     6462F2F0 0 00000001 service-type(253) 4 2
     6462F304 0 00000001 Framed-Protocol(66) 4 1
     6462F318 0 00000009 policy-directive(339) 29 apply service internet_bronze
Profile: .*internet*
Updated: 00:00:33
Parse User: Y
Authen User: Y
     64630088 0 00000001 service-type(253) 4 5
     6463009C 0 00000009 ssg-service-info(350) 16 IBronze Internet
     646300B0 0 00000001 timeout(313) 4 90(5A)
```

```
-------------------------------------------------------
 Entries in Profile dB SG1 for regexp match
-------------------------------------------------------
Profile: .*internet*,
Updated: 00:00:33
Parse User: Y
Authen User: Y
     64630088 0 00000001 service-type(253) 4 5
     6463009C 0 00000009 ssg-service-info(350) 16 IBronze Internet
     646300B0 0 00000001 timeout(313) 4 90(5A)
Profile: .*user*,
Updated: 00:00:34
Parse User: Y
Authen User: Y
     6462F2F0 0 00000001 service-type(253) 4 2
     6462F304 0 00000001 Framed-Protocol(66) 4 1
     6462F318 0 00000009 policy-directive(339) 29 apply service internet_bronze
```

Related Commands

Command	Description
clear aaa cache group	Clears individual entries or all entries in the cache.
debug aaa cache group	Debugs the caching mechanism and ensures that entries are being cached from AAA server responses and are being found when queried.

show aaa dead-criteria

To display dead-criteria detection information for an authentication, authorization, and accounting (AAA) server, use the **show aaa dead-criteria** command in privileged EXEC mode.

show aaa dead-criteria {**security-protocol** *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [*server-group-name*]

Syntax Description

security-protocol	Security protocol of the specified AAA server. Currently, the only protocol that is supported is RADIUS.
ip-address	IP address of the specified AAA server.
auth-port	(Optional) Authentication port for the RADIUS server that was specified.
port-number	(Optional) Number of the authentication port. The default is 1645 (for a RADIUS server).
acct-port	(Optional) Accounting port for the RADIUS server that was specified.
port-number	(Optional) Number of the accounting port. The default is 1646 (for a RADIUS server).
server-group-name	(Optional) Server group with which the specified server is associated. The default is “radius” (for a RADIUS server).

Defaults

Currently, the *port-number* argument for the **auth-port** keyword and the *port-number* argument for the **acct-port** keyword default to 1645 and 1646, respectively. The default for the *server-group-name* argument is radius.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(6)	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

Multiple RADIUS servers having the same IP address can be configured on a router. The **auth-port** and **acct-port** keywords are used to differentiate the servers. The dead-detect interval of a server that is associated with a specified server group can be obtained by using the **server-group-name** keyword. (The dead-detect interval and retransmit values of a RADIUS server are set on the basis of the server group to which the server belongs. The same server can be part of multiple server groups.)

Examples

The following example shows that dead-criteria-detection information has been requested for a RADIUS server at the IP address 172.19.192.80:

```
Router# show aaa dead-criteria radius 172.19.192.80 radius

RADIUS Server Dead Critieria:
```

```
============================
Server Details:
    Address : 172.19.192.80
    Auth Port : 1645
    Acct Port : 1646
Server Group : radius
Dead Criteria Details:
    Configured Retransmits : 62
    Configured Timeout : 27
    Estimated Outstanding Transactions: 5
    Dead Detect Time : 25s
    Computed Retransmit Tries: 22
    Statistics Gathered Since Last Successful Transaction
=====================================================
Max Computed Outstanding Transactions: 5
Max Computed Dead Detect Time: 25s
Max Computed Retransmits : 22
```

The “Max Computed Dead Detect Time” is displayed in seconds. The other fields shown in the display are self-explanatory.

Related Commands

Command	Description
debug aaa dead-criteria transactions	Displays AAA dead-criteria transaction values.
radius-server dead-criteria	Forces one or both of the criteria—used to mark a RADIUS server as dead—to be the indicated constant.
show aaa server-private	Displays the status of all private RADIUS servers.
show aaa servers	Displays information about the number of packets sent to and received from AAA servers.

show aaa local user lockout

To display a list of all locked-out users, use the **show aaa local user lockout** command in privileged EXEC mode.

show aaa local user lockout

Syntax Description

This command has no arguments or keywords.

Defaults

Names of locked-out users are not displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command can be used only by users having root privilege.

Examples

The following output of the **show aaa local user lockout** command illustrates that user1 is locked out:

```
Router# show aaa local user lockout

               Local-user          Lock time
               user1                  04:28:49 UTC Sat Jun 19 2004
```

The fields in the output example are self-explanatory.

Related Commands

Command	Description
aaa local authentication attempts max-fail	Specifies the maximum number of unsuccessful authentication attempts before a user is locked out.
clear aaa local user fail-attempts	Clears the unsuccessful login attempts of a user.
clear aaa local user lockout	Unlocks the locked-out user.

show aaa memory

To display the output of the AAA data structure memory tracing information, use the **show aaa memory** command in user EXEC or privileged EXEC mode.

show aaa memory [**detailed** [**component** [**line**]] | **stats** {**all** | **attr_list** | **cursor** | **event** | **request** | **summary**}]

Syntax Description

detailed	(Optional) Displays information about the status of various AAA data structures actively used by AAA clients and statistics of data structure usage.
component	(Optional) Displays information about a specified component.
line	(Optional) Displays the substring to match in the component name.
stats	(Optional) Displays data-structure memory statistics.
all	(Optional) Displays memory statistics.
attr_list	(Optional) Displays the attribute list usage statistics.
cursor	(Optional) Displays the cursor usage statistics.
event	(Optional) Displays the event usage statistics.
request	(Optional) Displays the request usage statistics.
summary	(Optional) Displays the data-structure usage summary.

Command Modes

User EXEC (>)
Privileged EXEC (#

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than IOS Release 12.4(24)T.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI. The **stats** keyword is not supported in this release.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC. The **stats** keyword is not supported in this release.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use the **show aaa memory** to display the status of various AAA data structures actively used by AAA clients and statistics of data structure usage.

Examples

The following is sample output from the **show aaa memory detailed** command:

```
Router# show aaa memory detailed

AAA (accounting)             In-use Asked-For/Allocated Count  Size  Cfg/Max
  ---------------------------------------------------------------------------
  aaa_acct_rec            :        --        --/--           --    72   --/--
```

```
  aaa_acct_rec_node       :        --        --/--           --    24   --/--

  AAA (attribute)              In-use Asked-For/Allocated Count  Size  Cfg/Max
  ------------------------------------------------------------------------------
  aaa_attr                :        --        --/--           --    16   --/--
  aaa_attr_list           :        --        --/--           --    20   --/--

  AAA (database)               In-use Asked-For/Allocated Count  Size  Cfg/Max
  ------------------------------------------------------------------------------
  hash_elt                :        --        --/--           --    64   --/--
  aaa_acct_db             :        --        --/--           --   160   --/--
  aaa_db_elt_chunk        :       128     61568/912           2    64 2048/0
  aaa_uid_hash_table_str  :      4096      4096/4148          1  4096   --/--
  Total                   :      4224     65664/5060          3    --   --/--

  AAA (misc)                   In-use Asked-For/Allocated Count  Size  Cfg/Max
  ------------------------------------------------------------------------------
  aaa_interface           :        --        --/--           --   280   --/--
  aaa_idb_name            :        --        --/--           --   232   --/--
  aaa_general_db          :        --        --/--           --   644   --/--
  aaa_chunks              :        --         0/0            --    28  200/0
  aaa_interface_struct    :       560       560/664          2   280   --/--
  Total                   :       560       560/664          2    --   --/--

  RADIUS                       In-use Asked-For/Allocated Count  Size  Cfg/Max
  ------------------------------------------------------------------------------

  Total allocated: 0.004 Mb, 5 Kb, 5724 bytes

AAA Low Memory Statistics:
__________________________
  Authentication low-memory threshold      : 3%
  Accounting low-memory threshold          : 2%


  AAA Unique ID Failure                    : 0
  Local server  Packet dropped             : 0
  CoA  Packet dropped                      : 0
  PoD  Packet dropped                      : 0
```

The following is sample output from the **show aaa memory stats all** command:

```
Router# show aaa memory stats all
AAA Memory trace summary:
-------------------------------------------------------------------------------
TYPE           mallocs        frees        failures        active      max-usage
-------------------------------------------------------------------------------
AAA_ATTR_L          41           40               0             1             6
AAA_CURSOR          88           88               0             0             2
AAA_EVENT            5            5               0             0             1
AAA_REQUES           2            2               0             0             1
-------------------------------------------------------------------------------

AAA_ATTR_LIST data-structure active allocations trace:
-------------------------------------------------------------------
  Allocator-PC            AAA API                 Active Mallocs
-------------------------------------------------------------------
 0x01956360     aaa_attr_list_alloc                          1
-------------------------------------------------------------------

AAA_CURSOR data-structure active allocations trace:
-------------------------------------------------------------------
  Allocator-PC            AAA API                 Active Mallocs
```

```
-----------------------------------------------------------------
-----------------------------------------------------------------

AAA_EVENT data-structure active allocations trace:
-----------------------------------------------------------------
  Allocator-PC            AAA API                 Active Mallocs
-----------------------------------------------------------------
-----------------------------------------------------------------

AAA_REQUEST data-structure active allocations trace:
-----------------------------------------------------------------
  Allocator-PC            AAA API                 Active Mallocs
-----------------------------------------------------------------
-----------------------------------------------------------------
```

Table 64 describes the significant fields in the display.

Table 64 show aaa memory stats all Field Descriptions

Field	Description
TYPE	AAA data structure type.
mallocs	Total number of data structures allocated.
frees	Total number of data structures freed.
failures	Total number of data structure allocations failed.
active	Total number of actively used data structures.
max-usage	Maximum number of active allocations of data structure at any point.

The following is sample output from the **show aaa memory stats** with the **attr_list** keyword:

```
Router# show aaa memory stats attr_list

AAA_ATTR_LIST data-structure active allocations trace:
-----------------------------------------------------------------
  Allocator-PC            AAA API                 Active Mallocs
-----------------------------------------------------------------
 0x01956360     aaa_attr_list_alloc                        1
-----------------------------------------------------------------
```

Table 65 describes the significant fields in the display.

Table 65 show aaa memory stats attr_list Field Descriptions

Field	Description
Allocator-PC	AAA client that allocated a active data structure
AAA API	AAA API called by the client for an actively allocated data structure.
Active Mallocs	Number of active allocations from a client PC.

The following is sample output from the **show aaa memory stats cursor** command:

```
Router# show aaa memory stats cursor

AAA_CURSOR data-structure active allocations trace:
-----------------------------------------------------------------
```

```
  Allocator-PC            AAA API                 Active Mallocs
-----------------------------------------------------------------
```

The following is sample output from the **show aaa memory stats event** command:

```
Router# show aaa memory stats event

AAA_EVENT data-structure active allocations trace:
-----------------------------------------------------------------
  Allocator-PC            AAA API                 Active Mallocs
-----------------------------------------------------------------
-----------------------------------------------------------------
```

The following is sample output from the **show aaa memory stats request** command:

```
Router# show aaa memory stats request

AAA_REQUEST data-structure active allocations trace:
-----------------------------------------------------------------
  Allocator-PC            AAA API                 Active Mallocs
-----------------------------------------------------------------
-----------------------------------------------------------------
```

show aaa method-lists

To display all the named method lists defined in the authentication, authorization, and accounting (AAA) subsystem, use the **show aaa method-lists** command in user EXEC or privileged EXEC mode.

show aaa method-lists {**accounting** | **all** | **authentication** | **authorization**}

Syntax Description

accounting	Displays method lists defined for accounting services.
all	Displays method lists defined for all services.
authentication	Displays method lists defined for authentication services.
authorization	Displays method lists defined for authorization services.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following example shows how to display method lists for the accounting services:

```
Router# show aaa method-lists accounting

acct queue=AAA_ML_ACCT_SHELL
name=Permanent None valid=TRUE id=0 Action=NOT_SET :state=ALIVE
acct queue=AAA_ML_ACCT_AUTH_PROXY
  name=default valid=TRUE id=0 Action=START STOP :state=DEAD : SERVER_GROUP tac+
acct queue=AAA_ML_ACCT_NET
  name=methodtest valid=TRUE id=BA000002 Action=START STOP :state=DEAD :
  name=tunnel valid=TRUE id=48000003 Action=START STOP :state=DEAD : SERVER_GROs
  name=session valid=TRUE id=5C000004 Action=START STOP :state=DEAD : SERVER_GRs
acct queue=AAA_ML_ACCT_CONN
acct queue=AAA_ML_ACCT_SYSTEM
  name= valid=TRUE id=82000005 Action=START STOP :state=DEAD : SERVER_GROUP rads
acct queue=AAA_ML_ACCT_RESOURCE
acct queue=AAA_ML_ACCT_RM
permanent lists
```

Table 66 describes the significant fields shown in the display.

Table 66 show aaa method-lists accounting Field Descriptions

Field	Description
acct queue	Specifies the type of service for which the method lists are defined.
name	Name of the method list for the specified AAA service.
valid	Indicates the validity of the method list.
id	A unique identifier for the specified AAA method list.
Action	Specifies the type of action to be performed on accounting records. One of the following types of actions is displayed: Start-stop, Stop-only or None.
state	Describes the current state of the AAA server. There are two possible states: • DEAD—Indicates that the server is currently presumed dead and, in the case of failovers, this server will be skipped unless it is the last server in the group. • ALIVE—Indicates that the server is currently considered alive and attempts will be made to communicate with it.
SERVER_GROUP	Name of the server group, RADIUS hosts or TACTACS+ hosts.

The following example shows how to display method lists for authentication services. Table 66 describes the significant fields shown in the display.

```
Router# show aaa method-lists authentication

authen queue=AAA_ML_AUTHEN_LOGIN
  name=default valid=TRUE id=0 :state=DEAD : SERVER_GROUP radius
authen queue=AAA_ML_AUTHEN_ENABLE
  name=default valid=TRUE id=0 :state=ALIVE : SERVER_GROUP tacacs+ ENABLE  NONE
authen queue=AAA_ML_AUTHEN_PPP
authen queue=AAA_ML_AUTHEN_SGBP
authen queue=AAA_ML_AUTHEN_ARAP
  name=default valid=TRUE id=0 :state=DEAD : SERVER_GROUP tacacs+
  name=MIS-access valid=TRUE id=FF000006 :state=DEAD : SERVER_GROUP tacacs+
authen queue=AAA_ML_AUTHEN_DOT1X
  name=default valid=TRUE id=0 :state=DEAD : SERVER_GROUP radius
authen queue=AAA_ML_AUTHEN_EAPOUDP
  name=default valid=TRUE id=0 :state=ALIVE : ENABLE  SERVER_GROUP radius
authen queue=AAA_ML_AUTHEN_8021X
permanent lists
  name=Permanent Enable None valid=TRUE id=0 :state=ALIVE : ENABLE  NONE
  name=Permanent Enable valid=TRUE id=0 :state=ALIVE : ENABLE
  name=Permanent None valid=TRUE id=0 :state=ALIVE : NONE
  name=Permanent Local valid=TRUE id=0 :state=ALIVE : LOCAL
```

The following example shows how to display method lists for authorization services. Table 66 describes the significant fields shown in the display.

```
Router# show aaa method-lists authorization

author queue=AAA_ML_AUTHOR_SHELL
author queue=AAA_ML_AUTHOR_NET
```

```
  name=method1 valid=TRUE id=12000001 :state=ALIVE : NONE
  name=mygroup valid=TRUE id=6D000007 :state=ALIVE : SERVER_GROUP radius LOCAL
  name=list11 valid=TRUE id=6C000009 :state=DEAD : SERVER_GROUP radius
author queue=AAA_ML_AUTHOR_CONN
  name=default valid=TRUE id=0 :state=ALIVE : SERVER_GROUP tacacs+
author queue=AAA_ML_AUTHOR_IPMOBILE
author queue=AAA_ML_AUTHOR_RM
author queue=AAA_ML_AUTHOR_CONFIG
author queue=AAA_ML_AUTHOR_AUTH_PROXY
  name=default valid=TRUE id=0 :state=ALIVE : SERVER_GROUP tacacs+
author queue=AAA_ML_AUTHOR_PREAUTH
author queue=AAA_ML_AUTHOR_FLTSV
  name=default valid=TRUE id=0 :state=DEAD : SERVER_GROUP grp1
name=group valid=TRUE id=48000008 :state=ALIVE : SERVER_GROUP tacacs+ NONE
permanent lists
  name=local-list valid=TRUE id=0 :state=ALIVE : LOCAL
```

The following example shows how to display method lists for all the services. Table 66 describes the significant fields shown in the display.

```
Router# show aaa method-lists all

authen queue=AAA_ML_AUTHEN_LOGIN
  name=default valid=TRUE id=0 :state=ALIVE : SERVER_GROUP tacacs+
authen queue=AAA_ML_AUTHEN_ENABLE
  name=default valid=TRUE id=0 :state=ALIVE : SERVER_GROUP tacacs+ ENABLE  NONE
authen queue=AAA_ML_AUTHEN_PPP
authen queue=AAA_ML_AUTHEN_SGBP
authen queue=AAA_ML_AUTHEN_ARAP
  name=default valid=TRUE id=0 :state=ALIVE : SERVER_GROUP tacacs+
  name=MIS-access valid=TRUE id=FF000006 :state=ALIVE : SERVER_GROUP tacacs+
authen queue=AAA_ML_AUTHEN_DOT1X
  name=default valid=TRUE id=0 :state=DEAD : SERVER_GROUP radius
authen queue=AAA_ML_AUTHEN_EAPOUDP
  name=default valid=TRUE id=0 :state=ALIVE : ENABLE  SERVER_GROUP radius
authen queue=AAA_ML_AUTHEN_8021X
permanent lists
  name=Permanent Enable None valid=TRUE id=0 :state=ALIVE : ENABLE  NONE
  name=Permanent Enable valid=TRUE id=0 :state=ALIVE : ENABLE
  name=Permanent None valid=TRUE id=0 :state=ALIVE : NONE
  name=Permanent Local valid=TRUE id=0 :state=ALIVE : LOCAL
author queue=AAA_ML_AUTHOR_SHELL
author queue=AAA_ML_AUTHOR_NET
  name=method1 valid=TRUE id=12000001 :state=ALIVE : NONE
  name=mygroup valid=TRUE id=6D000007 :state=ALIVE : SERVER_GROUP radius LOCAL
  name=list11 valid=TRUE id=6C000009 :state=DEAD : SERVER_GROUP radius
author queue=AAA_ML_AUTHOR_CONN
  name=default valid=TRUE id=0 :state=ALIVE : SERVER_GROUP tacacs+
author queue=AAA_ML_AUTHOR_IPMOBILE
author queue=AAA_ML_AUTHOR_RM
author queue=AAA_ML_AUTHOR_CONFIG
author queue=AAA_ML_AUTHOR_AUTH_PROXY
  name=default valid=TRUE id=0 :state=ALIVE : SERVER_GROUP tacacs+
author queue=AAA_ML_AUTHOR_PREAUTH
author queue=AAA_ML_AUTHOR_FLTSV
  name=default valid=TRUE id=0 :state=DEAD : SERVER_GROUP grp1
name=group valid=TRUE id=48000008 :state=ALIVE : SERVER_GROUP tacacs+ NONE
permanent lists
  name=local-list valid=TRUE id=0 :state=ALIVE : LOCAL
acct queue=AAA_ML_ACCT_SHELL
acct queue=AAA_ML_ACCT_AUTH_PROXY
  name=default valid=TRUE id=0 Action=START STOP :state=ALIVE : SERVER_GROUP ta+
acct queue=AAA_ML_ACCT_NET
```

```
  name=methodtest valid=TRUE id=BA000002 Action=START STOP :state=DEAD :
  name=tunnel valid=TRUE id=48000003 Action=START STOP :state=DEAD : SERVER_GROs
  name=session valid=TRUE id=5C000004 Action=START STOP :state=DEAD : SERVER_GRs
acct queue=AAA_ML_ACCT_CONN
acct queue=AAA_ML_ACCT_SYSTEM
  name= valid=TRUE id=82000005 Action=START STOP :state=DEAD : SERVER_GROUP rads
acct queue=AAA_ML_ACCT_RESOURCE
acct queue=AAA_ML_ACCT_RM
permanent lists
  name=Permanent None valid=TRUE id=0 Action=NOT_SET :state=ALIVE
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
aaa authentication arap	Enables a AAA authentication method for ARA.
aaa authorization	Sets parameters that restricts user access to a network.

show aaa service-profiles

To display the service profiles downloaded and stored by an authentication, authorization, and accounting (AAA) session, use the **show aaa service-profiles** command in user EXEC or privileged EXEC mode.

show aaa service-profiles

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Examples

The following is sample output from the **show aaa service-profiles** command. The field description is self-explantory.

```
Router# show aaa service-profiles

Service Name: example.com
```

Related Commands

Command	Description
aaa service-profiles	Configures the service profile parameters for a AAA session.

show aaa servers

To display the status and number of packets that are sent to and received from all public and private authentication, authorization, and accounting (AAA) RADIUS servers as interpretted by the AAA Server MIB, use the **show aaa servers** command in user EXEC or privileged EXEC mode.

show aaa servers [**private** | **public**]

Syntax Description

private	Displays private AAA servers only, which are also displayed by the AAA Server MIB.
public	Displays public AAA servers only, which are also displayed by the AAA Server MIB.

Command Modes

User EXEC or privileged EXEC

Command History

Release	Modification
12.2(6)T	This command was introduced.
12.3	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Only RADIUS servers are supported by the **show aaa servers** command.

The command displays information about packets sent and received for all AAA transaction types—authentication, authorization, and accounting.

Examples

The following is sample output from the **show aaa servers private** command. Only the first four lines of the display pertain to the status of private RADIUS servers, and the output fields in this part of the display are described in Table 67.

```
Router# show aaa servers private

RADIUS: id 24, priority 1, host 172.31.164.120, auth-port 1645,
acct-port 1646
      State: current UP, duration 18s, previous duration 0s
      Dead: total time 0s, count 0
      Authen: request 0, timeouts 0
              Response: unexpected 0, server error 0, incorrect 0, time 0ms
              Transaction: success 0, failure 0
      Author: request 0, timeouts 0
              Response: unexpected 0, server error 0, incorrect 0, time 0ms
              Transaction: success 0, failure 0
      Account: request 0, timeouts 0
              Response: unexpected 0, server error 0, incorrect 0, time 0ms
              Transaction: success 0, failure 0
      Elapsed time since counters last cleared: 2h1m
```

Table 67 describes the significant fields in the display.

Table 67 show aaa servers Field Descriptions

Field	Description
id	A unique identifier for all AAA servers defined on the router.
priority	The order of use for servers within a group.
host	IP address of the private RADIUS server host.
auth-port	User Datagram Protocol (UDP) destination port on the AAA server that is used for authentication and authorization requests. The default value is 1645.
acct-port	UDP destination port on the AAA server that is used for accounting requests. The default value is 1646.
State	Describes the current state of the AAA server; the duration, in seconds, that the server has been in that state; and the duration, in seconds, that the server was in the previous state. The following states are possible: • UP—Indicates that the server is currently considered alive and attempts will be made to communicate with it. • DEAD—Indicates that the server is currently presumed dead and, in the case of failovers, this server will be skipped unless it is the last server in the group. • duration—Is the amount of time the server is assumed to be in the current state, either UP or DEAD. • previous duration—Is the amount of time the server was considered to be in the previous state.
Dead	Indicates the number of times that this server has been marked dead, and the cumulative amount of time, in seconds, that it spent in that state.

Table 67 show aaa servers Field Descriptions (continued)

Field	Description
Authen	Provides information about authentication packets that were sent to and received from the server, and authentication transactions that were successful or that failed. The following information may be reported in this field: • request—Number of authentication requests that were sent to the AAA server. • timeouts—Number of timeouts (no responses) that were observed, when a transmission was sent to this server. • Response—Provides statistics about responses that were observed from this server and includes the following reports: – unexpected—Number of unexpected responses. A response is considered unexpected when it is received *after* the timeout period for the packet has expired. This may happen if the link to the server is severely congested, for example. An unexpected response can also be produced when a server generates a response for no apparent reason. – server error—Number of server errors. This category is a catch-all for error packets that do not fall into one of the previous categories. – incorrect—Number of incorrect responses. A response is considered incorrect if it is of the wrong format expected by the protocol. This frequently happens when an incorrect server key is configured on the router. • Transaction: These fields provide information about authentication, authorization, and accounting transactions related to the server. A transaction is defined as a request for authentication, authorization, or accounting information that is sent by the AAA module, or by an AAA client (such as PPP) to an AAA protocol (RADIUS or TACACS+), which may involve multiple packet transmissions and retransmissions. Transactions may require packet retransmissions to one or more servers in a single server group, to verify success or failure. Success or failure is reported to AAA by the RADIUS and TACACS+ protocols, as follows – success—Incremented when a transaction is successful. – failure—Incremented when a transaction fails (for example, packet retransmissions to another server in the server group failed due to failover or did not succeed. (A negative response to an Access-Request, such as Access-Reject, is considered to be a *successful* transaction).
Author	The fields in this category are similar to those in the Authen: fields. An important difference, however, is that because authorization information is carried in authentication packets for the RADIUS protocol, these fields are not incremented when using RADIUS.
Account	The fields in this category are similar to those in the Authen: fields, but provide accounting transaction and packet statistics.
Elapsed time since counters last cleared	Displays the amount of time in days, hours, and minutes that have passed since the counters were last cleared.

The fields in the output are mapped to Simple Network Management Protocol (SNMP) objects in the Cisco AAA-SERVER-MIB and are used in SNMP reporting. The first line of the report is mapped to the Cisco AAA-SERVER-MIB as follows:

- id maps to casIndex
- priority maps to casPriority
- host maps to casAddress
- auth-port maps to casAuthenPort
- acct-port maps to casAcctPort

Mapping the following set of objects listed in the Cisco AAA-SERVER-MIB map to fields displayed by the **show aaa servers** command is more straightforward. For example, the casAuthenRequests field corresponds to the Authen: request portion of the report, casAuthenRequestTimeouts corresponds to the Authen: timeouts portion of the report, and so on.

```
casStatisticsGroup OBJECT-GROUP
    OBJECTS{
        casAuthenRequests,
        casAuthenRequestTimeouts,
        casAuthenUnexpectedResponses,
        casAuthenServerErrorResponses,
        casAuthenIncorrectResponses,
        casAuthenResponseTime,
        casAuthenTransactionSuccesses,
        casAuthenTransactionFailures,
        casAuthorRequests,
        casAuthorRequestTimeouts,
        casAuthorUnexpectedResponses,
        casAuthorServerErrorResponses,
        casAuthorIncorrectResponses,
        casAuthorResponseTime,
        casAuthorTransactionSuccesses,
        casAuthorTransactionFailures,
        casAcctRequests,
        casAcctRequestTimeouts,
        casAcctUnexpectedResponses,
        casAcctServerErrorResponses,
        casAcctIncorrectResponses,
        casAcctResponseTime,
        casAcctTransactionSuccesses,
        casAcctTransactionFailures,
        casState,
        casCurrentStateDuration,
        casPreviousStateDuration,
        casTotalDeadTime,
        casDeadCount
    }
```

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:
http://www.cisco.com/go/mibs

Related Commands

Command	Description
radius-server dead-criteria	Forces one or both of the criteria—used to mark a RADIUS server as dead—to be the indicated constant.
server-private	Associates a particular private RADIUS server with a defined server group.

show aaa subscriber profile

To display all the subscriber profiles under the specified namestring in the authentication, authorization, and accounting (AAA) subsystem, use the **show aaa subscriber profile** command in user EXEC or privileged EXEC mode.

show aaa subscriber profile *profile-name*

Syntax Description

profile-name	The AAA subscriber profile name.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(31)SB1	This command was integrated into Cisco IOS Release 12.2(31)SB1.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command display all the subscriber profile CLIs under the specified namestring. If no namestring is specified, all the subscriber profiles in the subscriber profile database will be displayed.

Examples

The following example shows how to display subscriber profile information:

```
Router# show aaa subscriber profile db

-----------------------------------------------------------
 Entries in Profile dB subscribers for exact match
-----------------------------------------------------------
Profile: prof1
Updated: 00:00:55
Parse User: N
Authen User: N
Query Count: 4
     6897DBDC 0 0000000A service-name(381) 8 service1, service none, protocol ne
-----------------------------------------------------------
 Entries in Profile dB subscribers for regexp match
-----------------------------------------------------------
No entries found for regexp match
```

Table 66 describes the significant fields shown in the display.

Table 68 show aaa subscriber profile Descriptions

Field	Description
Profile	Indicates the subscriber profile specified.
Updated	Time elapsed since profile last updated.

Table 68 show aaa subscriber profile Descriptions (continued)

Field	Description
Parse User	Identifies this entry as a regexp.
Authen User	Identifies if entry matches require authentication.
Query Count	Usage Counters. Indicates the number of times Profile dB successfully found an entry when queried for.

Related Commands

Command	Description
aaa authorization subscriber-service	Configures local subscriber profiles which are used after the existing methods are exhausted.
subscriber profile	Configures service-related information under a particular subscriber profile.

show aaa user

To display attributes related to an authentication, authorization, and accounting (AAA) session, use the **show aaa user** command in privileged EXEC mode.

show aaa user {**all** | *unique id*}

Syntax Description

all	Displays information about all users for which AAA currently has knowledge.
unique id	Displays information for only this user.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

When a user logs into a Cisco router and uses AAA, a unique ID is assigned to the session. Throughout the life of the session, various attributes that are related to the session are collected and stored internally within a AAA database. These attributes can include the IP address of the user, the protocol being used to access the router (such as PPP or Serial Line Internet Protocol [SLIP]), the speed of the connection, and the number of packets or bytes that are received or transmitted.

The output of this command provides a snapshot of various subdatabases that are associated with a AAA unique ID. Some of the more important ones are listed in Table 68.

The output also shows various AAA call events that are associated with a particular session. For example, when a session comes up, the events generally recorded are CALL START, NET UP, and IP Control Protocol UP (IPCP UP).

In addition, the output provides a snapshot of the dynamic attributes that are associated with a particular session. (Dynamic attributes are those that keep changing values throughout the life of the session.) Some of the more important ones are listed in Table 68.

The unique ID of a session can be obtained from the output of the **show aaa sessions** command.

Note This command does not provide information for all users who are logged into a device, but for only those who have been authenticated or authorized using AAA or for only those whose sessions are being accounted for by the AAA module.

Note Using the **all** keyword can produce a large amount of output, depending on the number of users who are logged into the device at any given time.

Examples

The following example shows that information is requested for all users:

```
Router# show aaa user all
```

The following example shows that information is requested for user 5:

```
Router# show aaa user 5
```

The following is sample output from the **show aaa user** command. The session information displayed is for a PPP over Ethernet over Ethernet (PPPoEoE) session.

```
Router# show aaa user 3

Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *20:32:49.199 PST Wed Dec 17
2003

  Unique id 3 is currently in use.
  Accounting:
    log=0x20C201
    Events recorded :
      CALL START
      NET UP
      IPCP_PASS
      INTERIM START
      VPDN NET UP
  update method(s) :
    NONE
  update interval = 0
  Outstanding Stop Records : 0
  Dynamic attribute list:
    63CCF138 0 00000001 connect-progress(30) 4 LAN Ses Up
    63CCF14C 0 00000001 pre-session-time(239) 4 3(3)
    63CCF160 0 00000001 nas-tx-speed(337) 4 102400000(61A8000)
    63CCF174 0 00000001 nas-rx-speed(33) 4 102400000(61A8000)
    63CCF188 0 00000001 elapsed_time(296) 4 2205(89D)
    63CCF19C 0 00000001 bytes_in(97) 4 6072(17B8)
    63CCF1B0 0 00000001 bytes_out(223) 4 6072(17B8)
    63CCF1C4 0 00000001 pre-bytes-in(235) 4 86(56)
    63CCF1D8 0 00000001 pre-bytes-out(236) 4 90(5A)
    63CCF1EC 0 00000001 paks_in(98) 4 434(1B2)
    63CCF244 0 00000001 paks_out(224) 4 434(1B2)
    63CCF258 0 00000001 pre-paks-in(237) 4 7(7)
    63CCF26C 0 00000001 pre-paks-out(238) 4 9(9)
  No data for type EXEC
  No data for type CONN
  NET: Username=peer1
    Session Id=00000003 Unique Id=00000003
    Start Sent=1 Stop Only=N
    stop_has_been_sent=N
    Method List=63B4A10C : Name = default
    Attribute list:
    63CCF138 0 00000001 session-id(293) 4 3(3)
    63CCF14C 0 00000001 Framed-Protocol(62) 4 PPP
    63CCF160 0 00000001 protocol(241) 4 ip
    63CCF174 0 00000001 addr(5) 4 70.0.0.1
  No data for type CMD
  No data for type SYSTEM
  No data for type RM CALL
  No data for type RM VPDN
  No data for type AUTH PROXY
  No data for type IPSEC-TUNNEL
  No data for type RESOURCE
  No data for type 10
```

```
  No data for type CALL
Debg: No data available
Radi: 641AACAC
Interface:
  TTY Num = -1
  Stop Received = 0
  Byte/Packet Counts till Call Start:
    Start Bytes In = 106      Start Bytes Out = 168
    Start Paks    In = 3      Start Paks  Out = 4
  Byte/Packet Counts till Service Up:
    Pre Bytes In = 192      Pre Bytes Out = 258
    Pre Paks  In = 10      Pre Paks  Out = 13
  Cumulative Byte/Packet Counts :
    Bytes In = 6264      Bytes Out = 6330
    Paks  In = 444      Paks  Out = 447
  StartTime = 19:56:01 PST Dec 17 2003
  AuthenTime = 19:56:04 PST Dec 17 2003
  Component = PPoE
Authen: service=PPP type=CHAP method=RADIUS
Kerb: No data available
Meth: No data available
Preauth: No Preauth data.
General:
  Unique Id = 00000003
  Session Id = 00000003
  Attribute List:
    63CCF180 0 00000001 port-type(156) 4 PPP over Ethernet
    63CCF194 0 00000009 interface(152) 7 0/0/0/0
PerU: No data available
```

Table 68 lists the significant fields shown in the display.

Table 69 show aaa user Field Descriptions

Field	Description
EXEC	Exec-Accounting database
NET	Network Accounting database
CMD	Command Accounting database
Pre Bytes In	Bytes that were received before the call was authenticated
Pre Bytes Out	Bytes that were transmitted before the call was authenticated
Pre Paks In	Packets that were received before the call was authenticated
Pre Paks Out	Packets that were transmitted before the call was authenticated
Bytes In	Bytes that were received after the call was authenticated
Bytes Out	Bytes that were transmitted after the call was authenticated
Paks In	Packets that were received after the call was authenticated
Paks Out	Packets that were transmitted after the call was authenticated

Table 69 show aaa user Field Descriptions (continued)

Field	Description
Authen	Authentication database
General	General database
PerU	Per-User database

Related Commands

Command	Description
show aaa sessions	Displays information about AAA sessions as seen in the AAA Session MIB.

show access-group mode interface

To display the Access Control List (ACL) configuration on a Layer 2 interface, use the **show access-group mode interface** command in privileged EXEC mode.

show access-group mode interface [*interface interface-number*]

Syntax Description

type	(Optional) Interface type; valid values are **fastethernet**, **gigabitethernet**, **tengigabitethernet**, and **port-channel**.
number	(Optional) Interface number.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

The valid values for the port number depend on the chassis used.

Examples

This example shows how to display the ACL configuration mode on Fast Ethernet interface 6/1:

```
Router# show access-group mode interface fastethernet 6/1

Interface FastEthernet6/1:
   Access group mode is: merge
Router#
```

Related Commands

Command	Description
access-group mode	Specifies the override modes and the nonoverride modes.

show access-lists compiled

To display a table showing Turbo Access Control Lists (ACLs), use the **show access-lists compiled** command in user EXEC or privileged EXEC mode.

show access-lists compiled

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(6)S	This command was introduced.
12.1(1)E	This command was introduced for Cisco 7200 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(4)E	This command was implemented on the Cisco 7100 series routers.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.

Usage Guidelines

This command is used to display the status and condition of the Turbo ACL tables associated with each access list. The Turbo ACL feature processes access lists more expediently, providing faster functionality for routers equipped with the feature. The Turbo ACL feature compiles the ACLs into a set of lookup tables, while maintaining the first match requirements. Packet headers are used to access these tables in a small, fixed number of lookups, independently of the existing number of ACL entries. The memory usage is displayed for each table; large and complex access lists may require substantial amounts of memory. If the memory usage is greater than the memory available, you can disable the Turbo ACL feature so that memory exhaustion does not occur, but the acceleration of the access lists is not then enabled.

Examples

The following is partial sample output from the **show access-lists compiled** command:

```
Router# show access-lists compiled

Compiled ACL statistics:
12 ACLs loaded, 12 compiled tables
 ACL         State      Tables  Entries  Config  Fragment  Redundant  Memory
1           Operational    1        2        1         0          0      1Kb
2           Operational    1        3        2         0          0      1Kb
3           Operational    1        4        3         0          0      1Kb
4           Operational    1        3        2         0          0      1Kb
5           Operational    1        5        4         0          0      1Kb
9           Operational    1        3        2         0          0      1Kb
20          Operational    1        9        8         0          0      1Kb
21          Operational    1        5        4         0          0      1Kb
```

```
101         Operational    1       15        9         7          2      1Kb
102         Operational    1       13        6         6          0      1Kb
120         Operational    1        2        1         0          0      1Kb
199         Operational    1        4        3         0          0      1Kb
First level lookup tables:
Block      Use              Rows       Columns   Memory used
  0   TOS/Protocol            6/16      12/16      66048
  1   IP Source (MS)         10/16      12/16      66048
  2   IP Source (LS)         27/32      12/16      132096
  3   IP Dest (MS)            3/16      12/16      66048
  4   IP Dest (LS)            9/16      12/16      66048
  5   TCP/UDP Src Port        1/16      12/16      66048
  6   TCP/UDP Dest Port       3/16      12/16      66048
  7   TCP Flags/Fragment      3/16      12/16      66048
```

Table 70 describes the significant fields shown in the display.

Table 70 show access-lists compiled Field Descriptions

Field	Description
State	Describes the state of each Turbo ACL table. Operational—The access list has been compiled by the Turbo ACL feature, and matching to this access list is performed through the Turbo ACL tables at high speed. Other possible values in the State field are as follows: • Unsuitable—The access list is not suitable for compiling, perhaps because it has time-range enabled entries, evaluate references, or dynamic entries. • Deleted—No entries are in this access list. • Building—The access list is being compiled. Depending on the size and complexity of the list, and the load on the router, the building process may take a few seconds. • Out of memory—An access list cannot be compiled because the router has exhausted its memory.
Entries	Number of ACL entries being used for the compilation. This number is effectively (Config + Fragment - Redundant).
Config	Number of ACL lines from the configuration itself.
Fragment	In order to handle IP fragments for entries that have Layer 4 information in them (for example, TCP port numbers), TurboACL generates extra ACL entries that match only IP fragments. These are used in the compilation, but do not appear in the configuration.
Redundant	Number of entries that are covered by an earlier entry, and therefore are redundant. These entries are not used in the compilation. Redundant entries come mainly from two sources; the config itself might contain redundant entries, often as a result of a poorly maintained, large ACL. More typically, when TurboACL adds extra entries for IP fragments, often these entries are redundant because other added fragment entries cover them.

Related Commands

Command	Description
access-list compiled	Enables the Turbo ACL feature.
access-list (extended)	Provides extended access lists that allow more detailed access lists.
access-list (standard)	Creates a standard access list.
clear access-list counters	Clears the counters of an access list.
clear access-temp	Manually clears a temporary access list entry from a dynamic access list.
ip access-list	Defines an IP access list by name.
show ip access-lists	Displays the contents of all current IP access lists.

show access-lists

To display the contents of current access lists, use the **show access-lists** command in user EXEC or privileged EXEC mode.

show access-lists [*access-list-number* | *access-list-name*]

Syntax Description

access-list-number	(Optional) Number of the access list to display. The system displays all access lists by default.
access-list-name	(Optional) Name of the IP access list to display.

Defaults

The system displays all access lists.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(6)S	The output was modified to identify the compiled ACLs.
12.1(1)E	This command was implemented on the Cisco 7200 series.
12.1(5)T	The command output was modified to identify compiled ACLs.
12.1(4)E	This command was implemented on the Cisco 7100 series.
12.2(2)T	The command output was modified to show information for IPv6 access lists.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show access-lists** command is used to display the current ACLs operating in the router. Each access list is flagged using the Compiled indication if it is operating as an accelerated ACL.

The display also shows how many packets have been matched against each entry in the ACLs, enabling the user to monitor the particular packets that have been permitted or denied. This command also indicates whether the access list is running as a compiled access list.

Examples

The following is sample output from the **show access-lists** command when access list 101 is specified:

```
Router# show access-lists 101

Extended IP access list 101
```

```
    permit tcp host 198.92.32.130 any established (4304 matches) check=5
    permit udp host 198.92.32.130 any eq domain (129 matches)
    permit icmp host 198.92.32.130 any
    permit tcp host 198.92.32.130 host 171.69.2.141 gt 1023
    permit tcp host 198.92.32.130 host 171.69.2.135 eq smtp (2 matches)
    permit tcp host 198.92.32.130 host 198.92.30.32 eq smtp
    permit tcp host 198.92.32.130 host 171.69.108.33 eq smtp
    permit udp host 198.92.32.130 host 171.68.225.190 eq syslog
    permit udp host 198.92.32.130 host 171.68.225.126 eq syslog
    deny   ip 150.136.0.0 0.0.255.255 224.0.0.0 15.255.255.255
    deny   ip 171.68.0.0 0.1.255.255 224.0.0.0 15.255.255.255 (2 matches) check=1
    deny   ip 172.24.24.0 0.0.1.255 224.0.0.0 15.255.255.255
    deny   ip 192.82.152.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.122.173.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.122.174.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.239.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.240.0 0.0.7.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.248.0 0.0.3.255 224.0.0.0 15.255.255.255
```

An access list counter counts how many packets are allowed by each line of the access list. This number is displayed as the number of matches. Check denotes how many times a packet was compared to the access list but did not match.

The following is sample output from the **show access-lists** command when the Turbo Access Control List (ACL) feature is configured on all of the following access lists.

Note The permit and deny information displayed by the **show access-lists** command may not be in the same order as that entered using the **access-list** command.

```
Router# show access-lists

Standard IP access list 1 (Compiled)
    deny   any
Standard IP access list 2 (Compiled)
    deny   192.168.0.0, wildcard bits 0.0.0.255
    permit any
Standard IP access list 3 (Compiled)
    deny   0.0.0.0
    deny   192.168.0.1, wildcard bits 0.0.0.255
    permit any
Standard IP access list 4 (Compiled)
    permit 0.0.0.0
    permit 192.168.0.2, wildcard bits 0.0.0.255
```

The following is sample output from the **show access-lists** command that shows information for IPv6 access lists when IPv6 is configured on the network:

```
Router# show access-lists

IPv6 access list list2
     deny ipv6 FEC0:0:0:2::/64 any sequence 10
     permit ipv6 any any sequence 20
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.

Command	Description
clear access-list counters	Clears the counters of an access list.
clear access-template	Clears a temporary access list entry from a dynamic access list manually.
ip access-list	Defines an IP access list by name.
show ip access-lists	Displays the contents of all current IP access lists.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

show accounting

The **show accounting** command is replaced by the **show aaa user** command. See the **show aaa user** command for more information.

show appfw

To display application firewall policy information, use the **show appfw** command in user EXEC or privileged EXEC mode.

show appfw {**configuration** | **dns** [**cache** [**policy** *policy-name*]] | **name** *appfw-name*}

Syntax Description

configuration	Displays configuration information for configured policies.
dns	Displays IP addresses resolved by the Domain Name System (DNS) server of the applicable instant messenger application.
cache	(Optional) Displays IP addresses related to the DNS server.
policy	(Optional) Displays information for the specified policy.
policy-name	Name of the policy.
name	Displays information about the specified application firewall.
appfw-name	Name of an application firewall.

Command Default

If no policies are specified, information for all policies is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	This command was modified. The **dns** and **cache** keywords were added to support instant messenger traffic inspection.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **name** keyword and *appfw-name* argument were added.

Usage Guidelines

Use this command to display information regarding the application firewall policy configuration or the IP addresses of the DNS cache.

Use the **show appfw** command in conjunction with the **show ip inspect config** command to display the complete firewall configuration.

If you do not specify a policy using the **policy** *policy-name* option, the IP addresses gathered for all DNS names and policies are displayed.

Examples

This following output for the **show appfw configuration** command displays the configuration for the inspection rule “mypolicy,” which is applied to all incoming HTTP traffic on FastEthernet interface 0/0. In this example, all available HTTP inspection parameters have been defined.

```
Router# show appfw configuration
```

```
Application Firewall Rule configuration
  Application Policy name mypolicy
    Application http
      strict-http action allow alarm
      content-length minimum 0 maximum 1 action allow alarm
      content-type-verification match-req-rsp action allow alarm
      max-header-length request length 1 response length 1 action allow alarm
      max-uri-length 1 action allow alarm
      port-misuse default action allow alarm
      request-method rfc default action allow alarm
      request-method extension default action allow alarm
      transfer-encoding default action allow alarm
```

Table 71 describes the significant fields shown in the display.

Table 71 show appfw configuration Field Descriptions

Field	Description
Application Policy name	Name of the application policy.
strict-http action allow alarm	Allows HTTP messages to pass through the firewall.
content-length minimum 0 maximum 1 action allow alarm	Allows HTTP traffic having the maximum message size of 1 to pass through the firewall.
content-type-verification match-req-rsp action allow alarm	Allows HTTP traffic after verifying the content type of the HTTP response against the accept field of the HTTP request.
max-header-length request length 1 response length 1 action allow alarm	Allows the alarm to pass through the firewall if both the maximum header length request and the response is 1.
max-uri-length 1 action allow alarm	Allows HTTP traffic if the uniform resource identifier (URI) length in the request message is 1.
port-misuse default action allow alarm	Allows HTTP traffic through the firewall for all the default applications in the HTTP message.
request-method rfc default action allow alarm	Allows HTTP traffic for RFC 2616 supported methods.
request-method extension default action allow alarm	Allows HTTP traffic for all the extension methods.
transfer-encoding default action allow alarm	Allows HTTP traffic for all types of transfer encoded messages.

Related Commands

Command	Description
show ip inspect config	Displays firewall configuration and session information.

show ase

Note Effective with Cisco IOS Release 12.4(24), the **show ase** command is not available in Cisco IOS software.

To display the Automatic Signature Extraction (ASE) run-time status or detected signatures, use the **show ase** command in privileged EXEC mode.

show ase [**dispersion-table** *num-entries-to-display* | **prevalence-table** *num-entries-to-display* | **signatures** | **special-case-table** *num-entries-to-display* | **statistics**]

Syntax Description

dispersion-table	(Optional) Displays the dispersion table.
num-entries-to-display	(Optional) The number of table entries to be displayed. The range is from 0 to 4294967295.
prevalence-table	(Optional) Displays the prevalence table.
signatures	(Optional) Displays the detected ASE signatures.
special-case-table	(Optional) Displays the special case table.
statistics	(Optional) Displays the address description table staistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(24)	This command was removed.

Usage Guidelines

Use the **show ase** command without any keywords to display the run-time status. Use the **show ase** command with the **signatures** keyword to display the detected ASE signatures.

This command is used on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors.

Examples

The following example output displays the ASE run-time status:

Note The ASE collector must be started in order for the ASE run-time status information to be displayed.

```
Router# show ase

ASE Information:

Collector IP: 10.10.10.3
TIDP Group  : 10
Status      : Online
```

```
Packets inspected: 1105071
Address Dispersion Threshold: 20
Prevalence Threshold: 10
Sampling set to: 1 in 64
Address Dispersion Inactivity Timer: 3600s
Prevalence Table Refresh Time: 60s
```

Table 72 describes the significant fields shown in the display.

Table 72 show ase Field Descriptions

Field	Description
Collector IP	The IP address of the ASE collector.
TIDP Group	Threat Information Distribution Protocol (TIDP) group used for exchange between the ASE sensor and ASE collector.
Status	The four states are: • Connected—The ASE sensor has connected with the ASE collector, but it has not completed initialization. • Enabled—The ASE feature is enabled in global configuration mode, but the ASE sensor has not connected with the ASE collector. • Not Enabled—The ASE feature is not enabled in global configuration mode. • Online—The ASE is ready for inspecting traffic.
Packets inspected	Total number of packets inspected on this ASE collector.
Address Dispersion Threshold	Number of IP address occurrences that are permitted by the ASE sensor before this signature is considered an anomaly. **Note** The Address Dispersion Threshold is configured on the ASE collector. This information is shown on the ASE sensor (this router) for informational purposes.
Prevalence Threshold	The number of signature occurrences that are permitted before this signature is considered an anomaly. The default threshold is 10 seconds.
Sampling set to	A sampling value that sets the chance for which a signature is being inspected. For example, 1 in 64 is less than 1 in 32 chances.
Address Dispersion Inactivity Timer	Number of seconds that a signature does not occur. After this interval elapses, the signature is purged from the Address Dispersion table.
Prevalence Table Refresh Time	Number of seconds that the ASE sensor has before it clears the occurrence table. If a signature does not occur for the Prevalence Threshold during a refresh, then the Prevalence Threshold is not considered.

The following example output displays the detected ASE signatures:

```
Router# show ase signature
```

```
Automatic Signature Extraction Detected Signatures
==================================================

Signature Hash: 0x1E4A2076AAEA19B1, Offset: 54, Dest Port: TCP 135,
Signature: 05 00 00 03 10 00 00 00 F0 00 10 00 01 00 00 00 B8 00 00 00 00 00 03 00 01 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
Signature Hash: 0x24EC60FB1CF9A800, Offset: 72, Dest Port: TCP 445,
Signature: 00 00 00 00 00 00 00 00 00 00 00 00 FF FE 00 00 00 00 00 62 00 02 50 43 20 4E
45 54 57 4F 52 4B 20 50 52 4F 47 52 41 4D
Signature Hash: 0x0B0275535FFF480C, Offset: 54, Dest Port: TCP 445,
Signature: 00 00 00 85 FF 53 4D 42 72 00 00 00 00 18 53 C8 00 00 00 00 00 00 00 00 00 00
00 00 00 00 FF FE 00 00 00 00 00 62 00 02
```

Related Commands

Command	Description
ase collector	Enters the ASE collector server IP address so that the ASE sensor has IP connectivity to the ASE collector.
ase group	Identifies the TIDP group number for the ASE feature.
ase enable	Enables the ASE feature on a specified interface.
ase signature extraction	Enables the ASE feature globally on the router.
clear ase signature	Clears ASE signatures that were detected on the router.
debug ase	Provides error, log, messaging, reporting, status, and timer information.

show audit

To display the contents of an audit file, use the **show audit** command in privileged EXEC mode.

show audit [**filestat**]

Syntax Description

filestat	(Optional) Displays the rollover counter for the circular buffer and the number of messages that are received. The rollover counter, which indicates the number of times circular buffer has been overwritten, is reset when the audit filesize is changed (via the **audit filesize** command).

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)S	This command was introduced.
12.0(27)S	This feature was integrated into Cisco IOS Release 12.0(27)S.
12.2(25)S	The **filestat** keyword was added.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The audit file is a fixed file size in the disk file system. The audit file contains syslog messages (also known as hashes), which monitor changes that are made to your router. A separate hash is maintained for each of the following areas: running version, running configuration, startup configuration, file system, and hardware configuration. The **show audit** command will display any changes that are made to any of these areas.

Note Audit logs are enabled by default and cannot be disabled.

Examples

The following example is sample output from the **show audit** command:

```
Router# show audit

*Sep 14 18:37:31.535:%AUDIT-1-RUN_VERSION:Hash:
24D98B13B87D106E7E6A7E5D1B3CE0AD User:

*Sep 14 18:37:31.583:%AUDIT-1-RUN_CONFIG:Hash:
4AC2D776AA6FCA8FD7653CEB8969B695 User:

*Sep 14 18:37:31.595:%AUDIT-1-STARTUP_CONFIG:Hash:
95DD497B1BB61AB33A629124CBFEC0FC User:
```

```
*Sep 14 18:37:32.107:%AUDIT-1-FILESYSTEM:Hash:
330E7111F2B526F0B850C24ED5774EDE User:

*Sep 14 18:37:32.107:%AUDIT-1-HARDWARE_CONFIG:Hash:
32F66463DDA802CC9171AF6386663D20 User:
```

Table 73 describes the significant fields shown in the display.

Table 73 show audit Field Descriptions

Field	Description
`AUDIT-1-RUN_VERSION:Hash: 24D98B13B87D106E7E6A7E5D1B3CE0AD User:`	Running version, which is a hash of the information that is provided in the output of the **show version** command: running version, ROM information, BOOTLDR information, system image file, system and processor information, and configuration register contents.
`AUDIT-1-RUN_CONFIG:Hash: 4AC2D776AA6FCA8FD7653CEB8969B695 User:`	Running configuration, which is a hash of the running configuration.
`AUDIT-1-STARTUP_CONFIG:Hash: 95DD497B1BB61AB33A629124CBFEC0FC User:`	Startup configuration, which is a hash of the contents of the files on NVRAM, which includes the startup-config, private-config, underlying-config, and persistent-data.
`AUDIT-1-FILESYSTEM:Hash: 330E7111F2B526F0B850C24ED5774EDE User:`	File system, which is a hash of the dir information on all of the flash file systems, which includes bootflash and any other flash file systems on the router.
`AUDIT-1-HARDWARE_CONFIG:Hash:32F6646 3DDA802CC9171AF6386663D20 User:`	Hardware configuration, which is a hash of platform-specific information that is generally provided in the output of the **show diag** command.

Related Commands

Command	Description
audit filesize	Changes the size of the audit file.
audit interval	Changes the time interval that is used for calculating hashes.

show authentication interface

To display information about the Auth Manager for a given interface, use the **show authentication interface** command in privileged EXEC mode.

show authentication interface *type number*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
number	Interface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

Use the **show authentication interface** command to display information about the Auth Manager for a given interface.

Examples

The following is sample output from the **show authentication interface** command:

```
Switch# show authentication interface g1/0/23

Client list:
  MAC Address     Domain   Status         Handle      Interface
  000e.84af.59bd  DATA     Authz Success  0xE0000000  GigabitEthernet1/0/23

Available methods list:
  Handle  Priority  Name
  3        0        dot1x
Runnable methods list:
  Handle  Priority  Name
  3        0        dot1x
```

Table 74 describes the significant fields shown in the display. Other fields are self-explanatory.

Table 74 show authentication interface Field Descriptions

Field	Description
MAC Address	The MAC address of the client.
Domain	The domain of the client—either DATA or voice.

Table 74 show authentication interface Field Descriptions (continued)

Field	Description
Status	The status of the authentication session. The possible values are: • Authc Failed—an authentication method has run for this session and authentication failed. • Authc Success—an authentication method has run for this session and authentication was successful. • Authz Failed—a feature has failed and the session has terminated. • Authz Success—all features have been applied to the session and the session is active. • Idle—this session has been initialized but no authentication methods have run. This is an intermediate state. • No methods—no authentication method has provided a result for this session. • Running—an authentication method is running for this session.
Interface	The type and number of the authentication interface.
Available methods list	Summary information for the authentication methods available on the interface.
Runnable methods list	Summary information for the authentication methods that can run on the interface.

Related Commands

Command	Description
show authentication registrations	Displays information about the authentication methods that are registered with the Auth Manager.
show authentication sessions	Displays information about the current Auth Manager sessions.

show authentication registrations

To display information about the authentication methods that are registered with the Auth Manager, use the **show authentication registrations** command in privileged EXEC mode.

show authentication registrations

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

Use the **show authentication registrations** command to display information about all methods registered with the Auth Manager.

Examples

The following is sample output for the show authentication registrations command:

```
Switch# show authentication registrations

Auth Methods registered with the Auth Manager:
   Handle    Priority   Name
     3          0       dot1x
     2          1       mab
     1          2       webauth
```

Table 75 describes the significant fields shown in the display.

Table 75 show authentication registrations Field Descriptions

Field	Description
Priority	The priority of the method. If the priority for authentication methods has not been configured with the **authentication priority** command, then the default priority is displayed. The default from highest to lowest is dot1x, mab, and webauth.
Name	The name of the authentication method. The values can be dot1x, mab, or webauth.

Related Commands

Command	Description
show authentication interface	Displays information about the Auth Manager for a given interface.
show authentication sessions	Displays information about current Auth Manager sessions.

show authentication sessions

To display information about current Auth Manager sessions, use the **show authentication sessions** command in privileged EXEC mode.

Note Effective with Cisco IOS Release 12.2(33)SXI, the **show dot1x** command is supplemented by the **show authentication** command. The **show dot1x** command is reserved for displaying output specific to the use of the 802.1X authentication method. The **show authentication sessions** command has a wider remit of displaying information for all authentication methods and authorization features.

show authentication sessions [**handle** *handle-id*] [**interface** *type number*] [**mac** *mac-address*] [**method** *method-name* [**interface** *type number*]] [**session-id** *session-id*]

Syntax Description

handle *handle-id*	(Optional) Specifies the particular handle for which Auth Manager information is to be displayed.
interface *type number*	(Optional) Specifies a particular interface type and number for which Auth Manager information is to be displayed.
mac *mac-address*	(Optional) Specifies the particular MAC address for which you want to display information.
method *method-name*	(Optional) Specifies the particular authentication method for which Auth Manager information is to be displayed. If you specify a method (**dot1x**, **mab**, or **webauth**), you may also specify an interface.
session-id *session-id*	(Optional) Specifies the particular session for which Auth Manager information is to be displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	Support for this command was introduced.
12.2(33)SXI	This command was changed to add the **handle** *handle* keyword and argument and add information to the output.

Usage Guidelines

Use the **show authentication sessions** command to display information about all current Auth Manager sessions. To display information about specific Auth Manager sessions, use one or more of the keywords.

Table 1-76 shows the possible operating states for the reported authentication sessions.

Table 1-76 Authentication Method States

State	Description
Not run	The method has not run for this session.
Running	The method is running for this session.
Failed over	The method has failed and the next method is expected to provide a result.

Table 1-76 Authentication Method States (continued)

State	Description
Success	The method has provided a successful authentication result for the session.
Authc Failed	The method has provided a failed authentication result for the session.

Table 1-77 shows the possible authentication methods.

Table 1-77 Authentication Method States

State	Description
dot1x	802.1X
mab	MAC authentication bypass
webauth	web authentication

Examples

The following example shows how to display all authentication sessions on the switch:

```
Router# show authentication sessions

Interface  MAC Address     Method   Domain   Status         Session ID
Gi1/48     0015.63b0.f676  dot1x    DATA     Authz Success  0A3462B1000000102983C05C
Gi1/5      000f.23c4.a401  mab      DATA     Authz Success  0A3462B10000000D24F80B58
Gi1/5      0014.bf5d.d26d  dot1x    DATA     Authz Success  0A3462B10000000E29811B94
```

The following example shows how to display all authentication sessions on an interface:

```
Router# show authentication sessions interface gigabitethernet2/47

Interface:  GigabitEthernet2/47
          MAC Address:  Unknown
           IP Address:  Unknown
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  multi-host
     Oper control dir:  both
        Authorized By:  Guest Vlan
          Vlan Policy:  20
       Session timeout:  N/A
          Idle timeout:  N/A
    Common Session ID:  0A3462C8000000000002763C
      Acct Session ID:  0x00000002
                Handle:  0x25000000

Runnable methods list:
       Method   State
       mab      Failed over
       dot1x    Failed over

---------------------------------------

            Interface:  GigabitEthernet2/47
          MAC Address:  0005.5e7c.da05
           IP Address:  Unknown
            User-Name:  00055e7cda05
               Status:  Authz Success
               Domain:  VOICE
```

```
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3462C8000000010002A238
      Acct Session ID:  0x00000003
               Handle:  0x91000001

Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

The following example shows how to display the authentication session for a specified session ID:

```
Router# show authentication sessions session-id 0B0101C70000004F2ED55218

            Interface:  GigabitEthernet9/2
          MAC Address:  0000.0000.0011
           IP Address:  20.0.0.7
             Username:  johndoe
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  multi-host
     Oper control dir:  both
        Authorized By:  Critical Auth
          Vlan policy:  N/A
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0B0101C70000004F2ED55218
      Acct Session ID:  0x00000003
               Handle:  0x91000001

Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

The following examples show how to display all clients authorized by the specified authentication method:

```
Router# show authentication sessions method mab

No Auth Manager contexts match supplied criteria

Router# show authentication sessions method dot1x

Interface  MAC Address     Domain   Status         Session ID
Gi9/2      0000.0000.0011  DATA     Authz Success  0B0101C70000004F2ED55218
```

Table 74 describes the significant fields shown in the display.

Table 78 show authentication sessions Field Descriptions

Field	Description
MAC Address	The MAC address of the client.
Domain	The name of the domain, either DATA or VOICE.

Table 78 show authentication sessions Field Descriptions (continued)

Field	Description
Status	The status of the authentication session. The possible values are: • Authc Failed—an authentication method has run for this session and authentication failed. • Authc Success—an authentication method has run for this session and authentication was successful. • Authz Failed—a feature has failed and the session has terminated. • Authz Success—all features have been applied to the session and the session is active. • Idle—this session has been initialized but no authentication methods have run. This is an intermediate state. • No methods—no authentication method has provided a result for this session. • Running—an authentication method is running for this session.
Handle	The context handle.
Interface	The type and number of the authentication interface.

Related Commands

Command	Description
show authentication interface	Displays information about the status of controlled ports.
show authentication registrations	Displays information about the authentication methods that are registered with the Auth Manager.
show dot1x	Displays details for an identity profile specific to the use of the 802.1X authentication method.

show auto secure config

To display AutoSecure configurations, use the **show auto secure config** command in privileged EXEC mode.

show auto secure config

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.
12.3(15)	Autosecure disables the configuration of the autosec_iana_reserved_block, autosec_private_block, or autosec_complete_bogon access control lists (acls), and application-to-edge interfaces. Output for these acls is no longer shown in the show output.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Examples

The following sample output from the **show auto secure config** command shows what has been enabled and disabled via the **auto secure** command:

```
Router# show auto secure config

no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
security passwords min-length 6
security authentication failure rate 10 log
enable secret 5 $1$CZ6G$GkGOnHdNJCO3CjNHHyTUA.
aaa new-model
aaa authentication login local_auth local
line console 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line aux 0
 login authentication local_auth
 exec-timeout 10 0
 transport output telnet
```

```
line vty 0 4
 login authentication local_auth
 transport input telnet
ip domain-name cisco.com

crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
 transport input ssh telnet
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
interface FastEthernet0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
!
interface FastEthernet1/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
!
interface FastEthernet1/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
!
interface FastEthernet0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
!
ip cef
interface FastEthernet0/0
 ip verify unicast reverse-path
ip inspect audit-trail
ip inspect dns-timeout 7
ip inspect tcp idle-time 14400
ip inspect udp idle-time 1800
ip inspect name autosec_inspect cuseeme timeout 3600
ip inspect name autosec_inspect ftp timeout 3600
ip inspect name autosec_inspect http timeout 3600
ip inspect name autosec_inspect rcmd timeout 3600
ip inspect name autosec_inspect realaudio timeout 3600
ip inspect name autosec_inspect smtp timeout 3600
ip inspect name autosec_inspect tftp timeout 30
ip inspect name autosec_inspect udp timeout 15
```

```
ip inspect name autosec_inspect tcp timeout 3600
access-list 100 deny ip any any
interface FastEthernet0/0
 ip inspect autosec_inspect out
 ip access-group 100 in
```

Related Commands

Command	Description
auto secure	Secures the management and forwarding planes of the router.

show call admission statistics

To monitor the global Call Admission Control (CAC) configuration parameters and the behavior of CAC, use the **show call admission statistics** command in user EXEC or privileged EXEC mode.

show call admission statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following is sample output from the **show call admission statistics** command:

```
Router# show call admission statistics

Total Call admission charges: 0, limit 25
Total calls rejected 12, accepted 51
Load metric: charge 0, unscaled 0
```

Table 79 describes the significant fields shown in the display.

Table 79 show call admission statistics Field Descriptions

Field	Description
Total call admission charges	Percentage of system resources being charged to the system. If you configured a resource limit, SA requests are dropped when this field is equal to that limit.
limit	Maximum allowed number of total call admission charges. Valid values are 0 to 100000.
Total calls rejected	Number of SA requests that were not accepted.
accepted	Number of SA requests that were accepted.
unscaled	Not related to IKE. This value always is 0.

Related Commands

Command	Description
call admission limit	Instructs IKE to drop calls when a specified percentage of system resources are being consumed.
crypto call admission limit	Specifies the maximum number of IKE SA requests allowed before IKE begins rejecting new IKE SA requests.

show class-map type inspect

To display Layer 3 and Layer 4 or Layer 7 (application-specific) inspect type class maps and their matching criteria, use the **show class-map type inspect** command in privileged EXEC mode.

show class-map type inspect [*protocol-name*] [*class-map-name*]

Syntax Description

protocol-name	(Optional) Layer 7 application-specific class map. The supported protocols are as follows: • **aol**—America Online Instant Messenger (IM) • **edonkey**—eDonkey peer-to-peer (P2P) • **fasttrack**—FastTrack traffic P2P • **gnutella**—Gnutella Version 2 traffic P2P • **h323**—H323 protocol • **http**—HTTP • **icq**—I Seek You (ICQ) IM • **imap**—Internet Message Access Protocol (IMAP) • **kazaa2**—Kazaa Version 2 P2P • **msnmsgr**—MSN Messenger IM protocol • **pop3**—Post Office Protocol, Version 3 (POP 3) • **sip**—SMDS Interface Protocol (SIP) • **smtp**—Simple Mail Transfer Protocol (SMTP) • **sunrpc**—SUN Remote Procedure Call (SUNRPC) • **winmsgr**—Windows IM • **ymsgr**—Yahoo IM
class-map-name	(Optional) Name of the inspect type class map. The name can be a maximum of 40 alphanumeric characters.

Command Default

Information for all inspect type class maps is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(9)T	This command was modified. The following keywords were added: **edonkey**, **fasttrack**, **gnutella**, **kazaa2**, **aol**, **msnmsgr**, **ymsgr**.

Release	Modification
12.4(20)T	This command was modified. The following keywords were added: **icq** and **winmsgr**.
Cisco IOS XE Release 2.1	This command was modified. It was integrated into Cisco IOS XE Release 2.1. The *protocol-name* argument is not supported.

Usage Guidelines

Use the **show class-map type inspect** command to display class maps for a particular inspect type class map.

Examples

The following is sample output from the **show class-map type inspect** command with all class maps:

```
Router# show class-map type inspect

Class Map type inspect match-all classe0 (id 7)
   Match access-group  34

 Class Map type inspect match-all c1 (id 5)
   Match access-group  101
   Match protocol http

 Class Map type inspect match-all class1 (id 1)
   Match none
```

The following is sample output from the **show class-map type inspect** with the class map classe0 specified:

```
Router# show class-map type inspect classe0

 Class Map type inspect match-all classe0 (id 7)
   Match access-group  34
```

Table 80 describes the significant fields shown in the display.

Table 80 show class-map type inspect Field Descriptions

Field	Description
Class Map	Inspect type class maps being displayed. Output is displayed for each configured class map. The choice for implementing class matches (for example, match-all) appears next to the traffic class.
Match	Match criteria specified for the class map. For inspect type class maps without any protocols specified, the criteria are **access-group**, **class-map**, **protocol**, and **user-group**. For inspect type class maps with protocols specified, the criteria are **no** and **service**.

Related Commands

Command	Description
show class-map type port-filter	Displays port-filter class maps and their matching criteria.

show class-map type urlfilter

To display URL filter class maps and their matching criteria, use the **show class-map type urlfilter** command in privileged EXEC mode.

show class-map type urlfilter [**trend | n2h2 | websense**] [*class-map-name*]

Syntax Description

trend	(Optional) Specifies Trend Micro class maps.
n2h2	(Optional) Specifies SmartFilter class maps.
websense	(Optional) Specifies Websense class maps.
class-map-name	(Optional) Name of the URL filter class map.

Command Default

Information for all local URL filter class maps is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **show class-map type urlfilter** command to display all local URL filter class maps and their matching criteria. To display class maps for a particular URL filtering server type—Trend Micro, SmartFilter or Websense—include the appropriate keyword. To display the matching criteria for a particular class map, specify the class map name.

Examples

The following is sample output from the **show class-map type urlfilter** command when three local URL filtering class maps have been configured:

```
Router# show class-map type urlfilter

 Class Map type urlfilter match-any untrusted-domain-class (id 1)
  Match server-domain urlf-glob untrusted-domain-param

 Class Map type urlfilter match-any trusted-domain-class (id 2)
  Match server-domain urlf-glob trusted-domain-param

 Class Map type urlfilter match-any keyword-class (id 4)
  Match url-keyword urlf-glob keyword-param
```

The following is sample output from the **show class-map type urlfilter trend** command when one Trend Micro URL filtering class map has been configured:

```
Router# show class-map type urlfilter trend

 Class Map type urlfilter trend match-any drop-category (id 3)
```

```
  Match url category Adult-Mature-Content
  Match url category Gambling
  Match url category Personals-Dating
```

The following is sample output from the **show class-map type urlfilter websense** command:

```
Router# show class-map type urlfilter websense

 Class Map type urlfilter websense match-any websense-map (id 5)
  Match server-response any
```

Table 81 describes the significant fields shown in the display.

Table 81 show class-map type urlfilter Field Descriptions

Field	Description
Class Map	URL filtering class map being displayed. Output is displayed for each configured class map of the type of URL filtering specified—**trend**, **n2h2**, or **websense**. The default URL filtering type is **local**. The choice for implementing class matches (for example, match-any) appears next to the traffic class.
Match	Match criteria specified for the class map. For local URL filtering class maps, the criteria are **server-domain urlf-glob** parameter maps and the **url-keyword urlf-glob** parameter map. For Trend-Micro URL filtering class maps, the criteria are **url-category** and **url-reputation**. For SmartFilter and Websense class maps, the match criterion is **server-response any**.

show crypto ace redundancy

To display information about a Blade Failure Group, use the **show crypto ace redundancy** command in privileged EXEC mode.

show crypto ace redundancy

Defaults

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)SXE2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows information about a Blade Failure Group that has a group ID of 1 and consists of two IPSec VPN SPAs—one IPSec VPN SPA is in slot 3, subslot 0 and one IPSec VPN SPA is in slot 5, subslot 0:

```
Router# show crypto ace redundancy
---------------------------------------
LC Redundancy Group ID            :1
Pending Configuration Transactions:0
Current State                     :OPERATIONAL
Number of blades in the group     :2
Slots
---------------------------------------
Slot:3 Subslot:0
Slot state:0x36
Booted
Received partner config
Completed Bulk Synchronization
Crypto Engine in Service
Rebooted 22 times
Initialization Timer not running
Slot:5 Subslot:0
Slot state:0x36
Booted
Received partner config
Completed Bulk Synchronization
Crypto Engine in Service
Rebooted 24 times
Initialization Timer not running

ACE B2B Group State:OPERATIONAL Event:BULK DONE
ACE B2B Group State:CREATED Event:CONFIG_DOWNLOAD_DONE
ACE B2B Group State:DELETED Event:CONFIG_DELETE
ACE B2B Group State:OPERATIONAL Event:BULK DONE
```

```
ACE B2B Group State:CREATED Event:CONFIG_DOWNLOAD_DONE
ACE B2B Group State:DELETED Event:CONFIG_DELETE
ACE B2B Group State:OPERATIONAL Event:CONFIG_DOWNLOAD_DONE
ACE B2B Group State:DELETED Event:CONFIG_ADD
ACE B2B Group State:CREATED Event:UNDEFINED B2B HA EVENT
ACE B2B Group State:CREATED Event:CONFIG_DOWNLOAD_DONE
```

Related Commands

Command	Description
linecard-group feature card	Assigns a group ID to a Blade Failure Group.
redundancy	Enters redundancy configuration mode.
show redundancy linecard-group	Displays the components of a Blade Failure Group.

show crypto ca certificates

Note This command was replaced by the **show crypto pki certificates** command effective with Cisco IOS Release 12.3(7)T.

To display information about your certificate, the certification authority certificate, and any registration authority certificates, use the **show crypto ca certificates** command in privileged EXEC mode.

show crypto ca certificates

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command shows information about the following certificates:

- Your certificate, if you have requested one from the CA (see the **crypto pki enroll** command)
- The certificate of the CA, if you have received the CA's certificate (see the **crypto pki authenticate** command)
- RA certificates, if you have received RA certificates (see the **crypto pki authenticate** command)

Examples

The following is sample output from the **show crypto ca certificates** command after you authenticated the CA by requesting the CA's certificate and public key with the **crypto pki authenticate** command:

```
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

The CA certificate might show Key Usage as "Not Set."

The following is sample output from the **show crypto ca certificates** command, and shows the router's certificate and the CA's certificate. In this example, a single, general purpose RSA key pair was previously generated, and a certificate was requested but not received for that key pair.

```
Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
    Serial Number: 04806682
  Status: Pending
  Key Usage: General Purpose
    Fingerprint: 428125BD A3419600 3F6C7831 6CD8FA95 00000000
```

```
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

Note that in the previous sample, the router's certificate Status shows "Pending." After the router receives its certificate from the CA, the Status field changes to "Available" in the **show** output.

The following is sample output from the **show crypto ca certificates** command, and shows two router's certificates and the CA's certificate. In this example, special usage RSA key pairs were previously generated, and a certificate was requested and received for each key pair.

```
Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: 428125BDA34196003F6C78316CD8FA95
  Key Usage: Signature

Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: AB352356AFCD0395E333CCFD7CD33897
  Key Usage: Encryption

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

The following is sample output from the **show crypto ca certificates** command when the CA supports an RA. In this example, the CA and RA certificates were previously requested with the **crypto ca authenticate** command.

```
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set

RA Signature Certificate
  Status: Available
  Certificate Serial Number: 34BCF8A0
  Key Usage: Signature

RA KeyEncipher Certificate
  Status: Available
  Certificate Serial Number: 34BCF89F
  Key Usage: Encryption
```

Related Commands

Command	Description
crypto pki authenticate	Authenticates the CA (by obtaining the certificate of the CA).
crypto pki enroll	Obtains the certificates of your router from the CA.
debug crypto pki messages	Displays debug messages for the details of the interaction (message dump) between the CA and the route.
debug crypto pki transactions	Displays debug messages for the trace of interaction (message type) between the CA and the router.

show crypto ca crls

Note This command was replaced by the **show crypto pki crls** command effective with Cisco IOS Release 12.3(7)T.

To display the current certificate revocation list (CRL) on router, use the **show crypto ca crls** command in privileged EXEC mode.

show crypto ca crls

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1	This command was introduced.

Examples

The following is sample output of the **show crypto ca crls** command:

```
Router# show crypto ca crls

          CRL Issuer Name:
              OU = sjvpn, O = cisco, C = us
              LastUpdate: 16:17:34 PST Jan 10 2002
              NextUpdate: 17:17:34 PST Jan 11 2002
              Retrieved from CRL Distribution Point:
                LDAP: CN = CRL1, OU = sjvpn, O = cisco, C = us
```

Related Commands

Command	Description
crypto pki crl request	Requests that a new CRL be obtained immediately from the CA.

show crypto ca roots

The **show crypto ca roots** command is replaced by the **show crypto ca trustpoints** command. See the **show crypto ca trustpoints** command for more information.

show crypto ca timers

Note This command was replaced by the **show crypto pki timers** command effective with Cisco IOS Release 12.3(8)T.

To display the status of the managed timers that are maintained by Cisco IOS for public key infrastructure (PKI), use the **show crypto ca timers** command in privileged EXEC mode.

show crypto ca timers

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.

Usage Guidelines

For each timer, this command displays the time remaining before the timer expires. It also associates trustpoint certification authorities (CAs), except for certificate revocation list (CRL) timers, by displaying the CRL distribution point.

Examples

The following example is sample output for the **show crypto ca timers** command:

```
Router# show crypto ca timers

PKI Timers
| 4d15:13:33.144
 | 4d15:13:33.144  CRL http://msca-root.cisco.com/CertEnroll/msca-root.crl
 |328d11:56:48.372  RENEW msroot
 | 6:43.201  POLL verisign
```

Related Commands

Command	Description
auto-enroll	Enables autoenrollment.
crypto pki trustpoint	Declares the CA that your router should use.

show crypto ca trustpoints

Note This command was replaced by the **show crypto pki trustpoints** command effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXD.

To display the trustpoints that are configured in the router, use the **show crypto pki trustpoints** command in privileged EXEC or user EXEC mode.

show crypto ca trustpoints

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)
User EXEC (>)

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

This command replaces the **show crypto ca roots** command. If you enter the **show crypto ca roots** command, the output will be written back as the **show crypto pki trustpoints** command.

Examples

The following is sample output from the **show crypto ca trustpoints** command:

```
Router# show crypto ca trustpoints

Trustpoint bo:
    Subject Name:
    CN = bomborra Certificate Manager
     O = cisco.com
     C = US
          Serial Number:01
    Certificate configured.
    CEP URL:http://bomborra
    CRL query url:ldap://bomborra
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the CA that your router should use.

show crypto call admission statistics

To monitor Crypto Call Admission Control (CAC) statistics, use the **show crypto call admission statistics** command in user EXEC or privileged EXEC mode.

show crypto call admission statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(3)T	This command was modified. The output of this command was updated to display information about IPsec SAs.

Usage Guidelines

Enter this command to display information about the Crypto CAC configuration parameters and their history, including statistics regarding the current security association (SA) count, SAs being negotiated, total new SA requests, the number of Internet Key Exchange (IKE) and IPsec SA requests accepted and rejected, and details regarding why requests were rejected.

Examples

The following is sample output from the **show crypto call admission statistics** command:

```
Router# show crypto call admission statistics

----------------------------------------------------------------------
               Crypto Call Admission Control Statistics
----------------------------------------------------------------------
System Resource Limit:      111 Max IKE SAs:     0 Max in nego:  1000
Total IKE SA Count:           0 active:          0 negotiating:     0
Incoming IKE Requests:        0 accepted:        0 rejected:        0
Outgoing IKE Requests:        0 accepted:        0 rejected:        0
Rejected IKE Requests:        0 rsrc low:        0 Active SA limit: 0
                                                   In-neg SA limit: 0
IKE packets dropped at dispatch:        0

Max IPSEC SAs:   111
Total IPSEC SA Count:           0 active:          0 negotiating:     0
Incoming IPSEC Requests:        0 accepted:        0 rejected:        0
Outgoing IPSEC Requests:        0 accepted:        0 rejected:        0

Phase1.5 SAs under negotiation:         0
```

Table 82 describes the significant fields shown in the display.

Table 82 show crypto call admission statistics Field Descriptions

Field	Description
System Resource Limit	Percentage of system resources that a router is using before IKE starts dropping all SA requests.
Max IKE SAs	Number of active IKE SA requests allowed on the router.
Total IKE SA Count	Number of IKE SAs.
active	Number of active SAs.
negotiating	Number of SA requests being negotiated.
Incoming IKE Requests	Number of incoming IKE SA requests.
Incoming IKE Requests accepted	Number of accepted IKE SA requests.
Incoming IKE Requests rejected	Number of rejected incoming IKE SA requests.
Outgoing IKE Requests	Number of outgoing IKE SA requests.
Outgoing IKE requests accepted	Number of accepted outgoing IKE SA requests.
Outgoing IKE requests rejected	Number of rejected outgoing IKE SA requests.
Rejected IKE Requests	Number of IKE requests that were rejected.
rsrc low	Number of IKE requests that were rejected because system resources were low or the preconfigured system resource limit was exceeded.
SA limit	Number of IKE SA requests that were rejected because the SA limit has been reached.
Incoming IPSEC Requests	Number of incoming IPsec SA requests.
Incoming IPSEC Requests accepted	Number of accepted IPsec SA requests.
Incoming IPSEC Requests rejected	Number of rejected incoming IPsec SA requests.
Outgoing IPSEC Requests	Number of outgoing IPsec SA requests.
Outgoing IPSEC requests accepted	Number of accepted outgoing IPsec SA requests.
Outgoing IPSEC requests rejected	Number of rejected outgoing IPsec SA requests.
Phase1.5 SAs	Number of negotiations in XAUTH or configuration exchange mode.

Related Commands

Command	Description
clear crypto call admission statistics	Clears the counters that track the number of accepted and rejected IKE SA requests.

show crypto ctcp

To display information about a Cisco Tunnel Control Protocol (cTCP) session, use the **show crypto ctcp** command in privileged EXEC mode.

show crypto ctcp [**peer** *ip-address*] [**detail**]

Syntax Description

peer	(Optional) Displays information about a specific peer.
ip-address	(Optional) IP address of the specific peer.
detail	(Optional) Displays information about the local TCP sequence number and the TCP sequence number of the packets for the peer.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.

Examples

The following **show** command output displays detailed information about a specific peer:

```
Router# show crypto ctcp peer 10.76.235.21 detail

    Remote                  Local                VRF                  Status

    10.76.235.21:3519       10.76.248.239:10000                       CTCP_ACK_R
                            LocalSeq#6807392F    RemoteSeq#010116C7
```

Table 83 provides information about significant fields in the display.

Table 83 show crypto ctcp Field Descriptions

Field	Description
Remote	IP address of the remote peer with which this cTCP session is set up.
Local	IP address of the server to which the cTCP packets are addressed.
VRF	Name of the Virtual Private Network routing and forwarding (VRF) instance to which this session belongs. If the VRF is blank, the global routing table is used.
Status	Status of the cTCP session. CTCP_ACK_R is a successful cTCP setup. Any other state indicates that cTCP is not yet set up or failed to be set up.
LocalSeq	Sequence number of the last Transmission Control Protocol (TCP) packet sent by the server on this connection.
RemoteSeq	Sequence number of the last TCP packet that was received by the peer on this connection.

Related Commands

Command	Description
crypto ctcp	Configures cTCP encapsulation for Easy VPN.

show crypto datapath

To display the counters that help troubleshoot an encrypted data path, use the **show crypto datapath** command in privileged EXEC mode.

show crypto datapath {**ipv4** | **ipv6**} {**realtime** | **snapshot**} {**all** | **non-zero**} [**error** | **internal** | **punt** | **success**]

Syntax Description

ipv4	Designate IPv4 is used in the network.
ipv6	Designate IPv6 is used in the network.
realtime	Displays the counters that capture traffic statistics as they occur.
snapshot	Displays the counters that capture traffic statistics as of a single point in time.
all	Display all counters.
non-zero	Display all counters that have at least one event recorded.
error	(Optional) Display the packet processing and dropped packet errors.
internal	(Optional) Track the movement of a packet from end to end across an encrypted data path.
punt	(Optional) Display the instances when the configured processing method failed, and an alternative was used.
success	(Optional) Display the interfaces where packets were successfully processed.

Command Default

The command defaults are:

- IP version: **ipv4**
- Counters: **all**
- Display time: **realtime**

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Use the **show crypto datapath counters** command to troubleshoot an encrypted data path.

Note Cisco recommends use of this command only for troubleshooting under the guidance of a Cisco TAC engineer.

You must specify the IP version used in the network. You can display all counters, only the counters that have recorded events, or one of these specific counters:

- Error counters track packet processing errors and associated packet drops. When a packet encounters an error, the first 64 bytes of that packet are stored in a buffer, to facilitate troubleshooting.
- Internal counters show the detailed movement of a packet, end to end, across an encrypted data path.
- Punt counters track instances when the configured packet processing method failed, and an alternative method was used. Because such instances might indicate a problem, it is useful to track them.
- Success counters help diagnose network performance problems. Frequently, although a network is configured for fast switching or CEF, packets are using a slower path. Success counters record the interfaces in the data path where packets were successfully processed and reveal the actual processing path.

You must also choose the display timeframe for the counters:

- The **realtime** option captures traffic statistics as they occur, and results in significant discrepancies between the first data reports and later data, because the counters increment with the traffic flow. This is the default option.
- The **snapshot** option captures traffic statistics as of a specific point in time, and results in a close match among all counts, because the counters do not increment with the continuing traffic flow.

Examples

The following example shows output from the **show crypto datapath** command. In this example, the **snapshot** option is specified for the timeframe, and only counters that have recorded events are displayed. The output of this command is intended for use by Cisco TAC engineers.

```
Router# show crypto datapath ipv4 snapshot non-zero

Success Statistics: Snapshot at 21:34:30 PST Mar 4 2006
  crypto check input core
    2nd round ok:            245      1st round ok:            118
  post crypto ip encrypt
    post encrypt ipflowok:   230
  crypto ceal post encrypt switch
    post encrypt ipflowok-2: 230
Error Statistics: Snapshot at 21:34:30 PST Mar 4 2006
Punt Statistics: Snapshot at 21:34:30 PST Mar 4 2006
  crypto ceal post decrypt switch
    fs to ps:                245
Internal Statistics: Snapshot at 21:34:30 PST Mar 4 2006
  crypto check input
    check input core not con 378      check input core consume 623

  crypto check input core
    came back from ce:       245      deny pak:                15

  crypto ipsec les fs
    not esp or ah:           1113
  post crypto ip decrypt
    decrypt switch:          245
  crypto decrypt ipsec sa check
    check ident success:     245
  crypto ceal post decrypt switch
    fs:                      245
  crypto ceal post decrypt fs
    les ip turbo fs:         245      tunnel ip les fs:        245
```

```
crypto ceal post decrypt ps
  proc inline:             245
crypto ceal punt to process inline
  coalesce:                245      simple enq:              245

crypto ceal post encrypt switch
  ps:                      230
crypto ceal post encrypt ps
  ps coalesce:             230      simple enq:              230

crypto engine ps vec
  ip encrypt:              230
crypto send epa packets
  ucast next hop:          230      ip ps send:              230
```

Related Commands

Command	Description
show monitor event-trace	Displays contents of error history buffers.

show crypto debug-condition

To display crypto debug conditions that have already been enabled in the router, use the **show crypto debug-condition** command in privileged EXEC mode.

show crypto debug-condition {[**peer**] [**connid**] [**spi**] [**fvrf**] [**gdoi-group** *groupname*] [**isakmp profile** *profile-name*] [**ivrf**] [**local** *ip-address*] [**unmatched**] [**username** *username*]}

Syntax Description

peer	(Optional) Displays debug conditions related to the peer. Possible conditions can include peer IP address, subnet mask, hostname, username, and group key.
connid	(Optional) Displays debug conditions related to the connection ID.
spi	(Optional) Displays debug conditions related to the security parameter index (SPI).
fvrf	(Optional) Displays debug conditions related to the front-door virtual private network (VPN) routing and forwarding (FVRF) instance.
gdoi-group *groupname*	(Optional) Displays debug conditions related to the Group Domain of Interpretation (GDOI) group filter. • The *groupname* value is the name of the GDOI group.
isakmp profile *profile-name*	(Optional) Displays debug conditions related to the Internet Security Association Key Management Protocol (ISAKMP) profile filter. • The *profile-name* value is the name of the profile filter.
ivrf	(Optional) Displays debug conditions related to the inside VRF (IVRF) instance.
local *ip-address*	(Optional) Displays debug conditions related to the local address debug condition filters. • The *ip-address* is the IP address of the local crypto endpoint.
unmatched	(Optional) Displays debug messages related to the Internet Key Exchange (IKE), IP Security (IPsec), or the crypto engine, depending on what was specified via the **debug crypto condition unmatched** [**engine** | **gdoi-group** | **ipsec** | **isakmp**] command.
username *username*	(Optional) Displays debug messages related to the AAA Authentication (Xauth) or public key infrastructure (PKI) and authentication, authorization, and accounting (AAA) username filter.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.4(11)T	The **gdoi-group** *groupname*, **isakmp profile** *profile-name*, **local** *ip-address*, and **username** *username* keywords and arguments were added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can specify as many filter values as specified via the **debug crypto condition** command. (You cannot specify a filter value that you did not use in the **debug crypto condition** command.)

Examples

The following example shows how to display debug messages when the peer IP address is 10.1.1.1, 10.1.1.2, or 10.1.1.3 and when the connection ID 2000 of crypto engine 0 is used. This example also shows how to enable global debug crypto CLIs and enable the **show crypto debug-condition** command to verify conditional settings.

```
Router# debug crypto condition connid 2000 engine-id 1
Router# debug crypto condition peer ipv4 10.1.1.1
Router# debug crypto condition peer ipv4 10.1.1.2
Router# debug crypto condition peer ipv4 10.1.1.3
Router# debug crypto condition unmatched
! Verify crypto conditional settings.
Router# show crypto debug-condition

Crypto conditional debug currently is turned ON
IKE debug context unmatched flag:ON
IPsec debug context unmatched flag:ON
Crypto Engine debug context unmatched flag:ON

IKE peer IP address filters:
10.1.1.1  10.1.1.2   10.1.1.3

Connection-id filters:[connid:engine_id]2000:1,
! Enable global crypto CLIs to start conditional debugging.
Router# debug crypto isakmp
Router# debug crypto ipsec
Router# debug crypto engine
```

The following example shows how to disable all crypto conditional settings via the **reset** keyword:

```
Router# debug crypto condition reset
! Verify that all crypto conditional settings have been disabled.
Router# show crypto debug-condition

Crypto conditional debug currently is turned OFF
IKE debug context unmatched flag:OFF
IPsec debug context unmatched flag:OFF
Crypto Engine debug context unmatched flag:OFF
```

Related Commands

Command	Description
debug crypto condition	Defines conditional debug filters.
debug crypto condition unmatched	Displays crypto conditional debug messages when context information is unavailable to check against debug conditions.

show crypto dynamic-map

To display a dynamic crypto map set, use the **show crypto dynamic-map** command in privileged EXEC mode.

show crypto dynamic-map [**tag** *map-name*]

Syntax Description

tag *map-name*	(Optional) Displays only the crypto dynamic map set with the specified *map-name*.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show crypto dynamic-map** command to view a dynamic crypto map set.

Examples

The following is sample output for the **show crypto dynamic-map** command:

```
Router# show crypto dynamic-map

Crypto Map Template"vpn1" 1
        ISAKMP Profile: vpn1-ra
        No matching address list set.
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                vpn1,
```

The following partial configuration was in effect when the above **show crypto dynamic-map** command was issued:

```
crypto dynamic-map vpn1 1
 set transform-set vpn1
 set isakmp-profile vpn1-ra
 reverse-route
```

Related Commands

Command	Description
show crypto map	Views the crypto map configuration.

show crypto eli

To display how many IKE-SAs and IPSec sessions are active and how many Diffie-Hellman keys are in use for each hardware crypto engine, use the **show crypto eli** in user EXEC or privileged EXEC mode.

show crypto eli

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.1(5)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS release 12.2(33)SXH.

Usage Guidelines

Use this command to obtain a snapshot of how many Internet Key Exchange (IKE) and IP Security (IPSec) sessions are active and how many Diffie-Hellman keys are in use for each hardware crypto engine. The **show crypto eli** command also allows you to see how far an ISA is from reaching its maximum limit.

Note IKE is a key management protocol standard that is used in conjunction with the IPSec standard. IPSec can be configured without IKE. However, IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard. When IKE is used with IPSec, IKE automatically negotiates the IPSec security associations (SAs).

(The eli component of the command calls the Encryption Layer Interface.)

Examples

The following is sample output for the **show crypto eli** command:

```
Router# show crypto eli

Encryption Layer :  ACTIVE
 Number of crypto engines = 2.

 Slot-3 crypto engine details.
 Capability-IPSec :No-IPPCP, 3DES, NoRSA

 IKE-Session   :    0 active,  2029 max, 0 failed
 DH-Key        :    0 active,  1014 max, 0 failed
 IPSec-Session :    0 active,  4059 max, 0 failed
```

```
 Slot-5 crypto engine details.
 Capability-IPSec :No-IPPCP, 3DES, NoRSA

 IKE-Session   :    0 active,  2029 max, 0 failed
 DH-Key        :    0 active,  1014 max, 0 failed
 IPSec-Session :    0 active,  4059 max, 0 failed
```

The following is sample output for the **show crypto eli** command for the IPSec VPN SPA:

```
Router# show crypto eli

>>Hardware Encryption : ACTIVE
>> Number of hardware crypto engines = 2
>>
>> CryptoEngine SPA-IPSEC-2G[3/0] details: state = Active
>> Capability      :
>>     IPSEC: DES, 3DES, AES, RSA
>>
>> IKE-Session   :     0 active, 16383 max, 0 failed
>> DH            :     0 active,  9999 max, 0 failed
>> IPSec-Session :     0 active, 65534 max, 0 failed
>>
>> CryptoEngine SPA-IPSEC-2G[3/1] details: state = Active
>> Capability      :
>>     IPSEC: DES, 3DES, AES, RSA
>>
>> IKE-Session   :     1 active, 16383 max, 0 failed
>> DH            :     0 active,  9999 max, 0 failed
>> IPSec-Session :     2 active, 65534 max, 0 failed
```

Table 84 describes significant fields shown in the display.

Table 84 show crypto eli summary Field Descriptions

Field	Description
active	The number of sessions that are active on a given hardware crypto engine.
max	The maximum number of sessions allowed for any given IKE, DH, or IPSec entry.
failed	The number of times that Cisco IOS software attempted to create more sessions than the number specified in “max.”

show crypto eng qos

To monitor and maintain low latency queueing (LLQ) for IPSec encryption engines, use the **show crypto eng qos** command in privileged EXEC mode.

show crypto eng qos

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(13)T	This command was introduced in Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show crypto eng qos** command to determine if QoS is enabled on LLQ for IPSec encryption engines.

Examples

The following example shows how to determine if LLQ for IPSec encryption engines is enabled:

```
Router# show crypto eng qos

crypto engine name: Multi-ISA Using VAM2
        crypto engine type: hardware
                      slot: 5
                  queuing: enabled
         visible bandwidth: 30000 kbps
                  llq size: 0
    default queue size/max: 0/64
      interface table size: 32

  FastEthernet0/0 (3), iftype 1, ctable size 16, input filter:ip
precedence 5
    class voice (1/3), match ip precedence 5
          bandwidth 500 kbps, max token 100000
          IN  match pkt/byte 0/0, police drop 0
          OUT match pkt/byte 0/0, police drop 0

  class default, match pkt/byte 0/0, qdrop 0
  crypto engine bandwidth:total 30000 kbps, allocated 500 kbps
```

The field descriptions in the above display are self-explanatory.

show crypto engine

To display a summary of the configuration information for the crypto engines, use the **show crypto engine** command in privileged EXEC mode.

show crypto engine {**accelerator** {**statistic** | **ring** {**control** | **packet** | **pool**}} | **brief** | **configuration** | **connections** {**active** | **dh** | **dropped-packet** | **flow**} | **qos** | **token** [**detail**]}

Syntax Description

accelerator	Displays crypto accelerator information.
statistic	Displays crypto accelerator statistic information.
ring	Displays crypto accelerator ring information.
control	Displays control ring information.
packet	Displays packet ring information.
pool	Displays pool ring information.
brief	Displays a summary of the configuration information for the crypto engine.
configuration	Displays the version and configuration information for the crypto engine.
connections	Displays information about the crypto engine connections.
active	Displays all active crypto engine connections.
dh	Displays crypto engine Diffie-Hellman table entries.
dropped-packet	Displays crypto engine dropped packets.
flow	Displays crypto engine flow table entries.
qos	Displays quality of service (QoS) information. • This keyword has a null output if any advanced integration module (AIM) except AIM-VPN/SSL-1 is used. The command-line interface (CLI) will accept the command, but there will be no output.
token	Displays the crypto token engine information.
detail	(Optional) Displays the detailed information of the crypto token engine.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2	This command was introduced on the Cisco 7200, RSP7000, and 7500 series routers.
12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4(4)T	IPv6 address information was added to command output.
12.4(9)T	AIM-VPN/SSL-3 encryption module information was added to command output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(22)T	The **token** and **detail** keywords were added.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2. The **accelerator**, **control, packet, pool, ring**, and **static** keywords were added.

Usage Guidelines

This command displays all crypto engines and displays the AIM-VPN product name.

If a hardware crypto engine does not support native Group Domain of Interpretation (GDOI) header preservation, the **show crypto engine connections active** output for Group Encrypted Transport VPN (GET VPN) IP security (IPsec) connections displays a disallowed IP address of 0.0.0.0 (see the **show crypto engine connections active** "Examples" section).

Examples

The following is sample output from the **show crypto engine brief** command shows typical crypto engine summary information:

```
Router# show crypto engine brief

crypto engine name:  Virtual Private Network (VPN) Module
        crypto engine type:  hardware
                     State:  Enabled
                  Location:  aim 0
    VPN Module in slot:  0
          Product Name:  AIM-VPN/SSL-3
     Software Serial #:  55AA
             Device ID:  001F - revision 0000
             Vendor ID:  0000
          Revision No:  0x001F0000
          VSK revision:  0
          Boot version:  255
           DPU version:  0
           HSP version:  3.3(18) (PRODUCTION)
          Time running:  23:39:30
               Compression:  Yes
                       DES:  Yes
                     3 DES:  Yes
                   AES CBC:  Yes (128,192,256)
                  AES CNTR:  No
     Maximum buffer length:  4096
          Maximum DH index:  3500
          Maximum SA index:  3500
        Maximum Flow index:  7000
      Maximum RSA key size:  2048


        crypto engine name:  Cisco VPN Software Implementation
        crypto engine type:  software
             serial number:  CAD4FCE1
      crypto engine state:  installed
     crypto engine in slot:  N/A
```

Table 85 describes the significant fields shown in the display.

Table 85 show crypto engine brief Field Descriptions

Field	Description
crypto engine name	Name of the crypto engine as assigned with the *key-name* argument in the **crypto key generate dss** command.
crypto engine type	If "software" is listed, the crypto engine resides in either the Route Switch Processor (RSP) (the Cisco IOS crypto engine) or in a second-generation Versatile Interface Processor (VIP2). If "crypto card" or "Encryption Service Adapter" (ESA) is listed, the crypto engine is associated with an ESA.
crypto engine state	The state "installed" indicates that a crypto engine is located in the given slot, but it is not configured for encryption. The state "dss key generated" indicates the crypto engine found in that slot has Digital Signature Standard (DSS) keys already generated.
crypto engine in slot	Chassis slot number of the crypto engine. For the Cisco IOS crypto engine, this is the chassis slot number of the RSP.

The following is sample output from **show crypto engine** command shows IPv6 information:

```
Router# show crypto engine connections

    ID Interface  Type  Algorithm           Encrypt  Decrypt IP-Address
     1 Et2/0      IPsec MD5                       0       46 FE80::A8BB:CCFF:FE01:2C02
     2 Et2/0      IPsec MD5                      41        0 FE80::A8BB:CCFF:FE01:2C02
     5 Tu0        IPsec SHA+DES                   0        0
3FFE:2002::A8BB:CCFF:FE01:2C02
     6 Tu0        IPsec SHA+DES                   0        0
3FFE:2002::A8BB:CCFF:FE01:2C02
  1001 Tu0        IKE   SHA+DES                   0        0
3FFE:2002::A8BB:CCFF:FE01:2C02
```

The following **show crypto engine** command output displays information for a situation in which a hardware crypto engine does not support native GDOI:

```
Router# show crypto engine connections active

Crypto Engine Connections

ID Interface     Type  Algorithm           Encrypt  Decrypt IP-Address
1079 Se0/0/0.10  IPsec AES+SHA                  0        0 0.0.0.0
1080 Se0/0/0.10  IPsec AES+SHA                  0        0 0.0.0.0
4364 <none>      IKE   SHA+3DES                 0        0
4381 <none>      IKE   SHA+3DES                 0        0
```

Related Commands

Command	Description
crypto engine accelerator	Enables the use of the onboard hardware accelerator for IPSec encryption.

show crypto engine accelerator logs

To display information about the last 32 CryptoGraphics eXtensions (CGX) Library packet processing commands and associated parameters sent from the VPN module driver to the VPN module hardware, use the **show crypto engine accelerator logs** command in privileged EXEC mode.

show crypto engine accelerator logs

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(1)XC	This command was introduced on the Cisco 1720 and Cisco 1750 platforms.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use this command when encrypted traffic is sent to the router and a problem with the encryption module is suspected. Use the **debug crypto engine accelerator logs** command to enable command logging *before* using this command.

Note The **show crypto engine accelerator logs** command is intended only for Cisco Systems TAC personnel to collect debugging information.

Examples

The following is sample output for the **show crypto engine accelerator logs** command:

```
Router# show crypto engine accelerator logs

Contents of packet log (current index = 20):

tag = 0x5B02, cmd = 0x5000
param[0] = 0x000E, param[1] = 0x57E8
param[2] = 0x0008, param[3] = 0x0000
param[4] = 0x0078, param[5] = 0x0004
param[6] = 0x142C, param[7] = 0x142C
param[8] = 0x0078, param[9] = 0x000C
tag = 0x5B03, cmd = 0x4100
param[0] = 0x000E, param[1] = 0x583C
param[2] = 0x0034, param[3] = 0x0040
param[4] = 0x00B0, param[5] = 0x0004
param[6] = 0x1400, param[7] = 0x1400
param[8] = 0x0020, param[9] = 0x000C
tag = 0x5C00, cmd = 0x4100
```

```
param[0] = 0x000E, param[1] = 0x57BC
param[2] = 0x0034, param[3] = 0x0040
param[4] = 0x00B0, param[5] = 0x0004
param[6] = 0x1400, param[7] = 0x1400
param[8] = 0x0020, param[9] = 0x000C
.
.
.
tag = 0x5A01, cmd = 0x4100
param[0] = 0x000E, param[1] = 0x593C
param[2] = 0x0034, param[3] = 0x0040
param[4] = 0x00B0, param[5] = 0x0004
param[6] = 0x1400, param[7] = 0x1400
param[8] = 0x0020, param[9] = 0x000C

Contents of cgx log (current index = 12):

cmd = 0x0074 ret = 0x0000
param[0] = 0x0010, param[1] = 0x028E
param[2] = 0x0039, param[3] = 0x0D1E
param[4] = 0x0100, param[5] = 0x0000
param[6] = 0x0000, param[7] = 0x0000
param[8] = 0x0000, param[9] = 0x0000
cmd = 0x0062 ret = 0x0000
param[0] = 0x0035, param[1] = 0x1BE0
param[2] = 0x0100, param[3] = 0x0222
param[4] = 0x0258, param[5] = 0x0000
param[6] = 0x0000, param[7] = 0x0000
param[8] = 0x0000, param[9] = 0x0000
cmd = 0x0063 ret = 0x0000
param[0] = 0x0222, param[1] = 0x0258
param[2] = 0x0000, param[3] = 0x0000
param[4] = 0x0000, param[5] = 0x0000
param[6] = 0x0000, param[7] = 0x020A
param[8] = 0x002D, param[9] = 0x0000
.
.
.
cmd = 0x0065 ret = 0x0000
param[0] = 0x0222, param[1] = 0x0258
param[2] = 0x0010, param[3] = 0x028E
param[4] = 0x00A0, param[5] = 0x0008
param[6] = 0x0001, param[7] = 0x0000
param[8] = 0x0000, param[9] = 0x0000
```

Related Commands

Command	Description
debug crypto engine acclerator logs	Enables logging of commands and associated parameters sent from the VPN module driver to the VPN module hardware using a debug flag.

show crypto engine accelerator ring

To display the contents and status of the control command, transmit packets, and receive packet rings used by the hardware accelerator crypto engine, use the **show crypto engine accelerator ring** command in privileged EXEC mode.

show crypto engine accelerator ring [**control** | **packet** | **pool**]

Syntax Description

control	(Optional) Number of control commands that are queued for execution by the hardware accelerator crypto engine are displayed.
packet	(Optional) Contents and status information for the transmit packet rings that are used by the hardware accelerator crypto engine are displayed.
pool	(Optional) Contents and status information for the receive packet rings that are used by the hardware accelerator crypto engine are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(3)XL	This command was introduced for the Cisco uBR905 cable access router.
12.2(2)XA	Support was added for the Cisco uBR925 cable access router.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented for the AIM-VPN/EPII and AIM-VPN/HPII on the following platforms: Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.
12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.3(4)T	The AIM-VPN/BPII was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.

Usage Guidelines

This command displays the command ring information.

If there were valid data in any of the rings, the ring entry would be printed.

Examples

The following example shows the command ring information:

```
Router# show crypto engine accelerator ring packet

PPQ RING:

cmd ring:head = 10 tail =10

result ring:head = 10 tail =10

destination ring:head = 10 tail =10
```

```
source ring:head = 10 tail =10

free ring:head = 0 tail =255
        00000000  071A96C5
        00000000  071A96C5
        00000001  071A9465
        00000001  071A9465
        00000002  071A9205
        00000002  071A9205
.
.
.
```

Related Commands

Command	Description
clear crypto engine accelerator counter	Resets the statistical and error counters for the hardware accelerator to zero.
crypto ca	Defines the parameters for the certification authority used for a session.
crypto cisco	Defines the encryption algorithms and other parameters for a session.
crypto dynamic-map	Creates a dynamic map crypto configuration for a session.
crypto engine accelerator	Enables the use of the onboard hardware accelerator for IPSec encryption.
crypto ipsec	Defines the IPSec SAs and transformation sets.
crypto isakmp	Enables and defines the IKE protocol and its parameters.
crypto key	Generates and exchanges keys for a cryptographic session.
crypto map	Creates and modifies a crypto map for a session.
debug crypto engine accelerator control	Displays each control command as it is given to the crypto engine.
debug crypto engine accelerator packet	Displays information about each packet sent for encryption and decryption.
show crypto engine accelerator sa-database	Displays the active (in-use) entries in the crypto engine SA database.
show crypto engine accelerator statistic	Displays the current run-time statistics and error counters for the crypto engine.
show crypto engine brief	Displays a summary of the configuration information for the crypto engine.
show crypto engine configuration	Displays the version and configuration information for the crypto engine.
show crypto engine connections	Displays a list of the current connections maintained by the crypto engine.

show crypto engine accelerator sa-database

To display active (in-use) entries in the platform-specific virtual private network (VPN) module database, use the **show crypto engine accelerator sa-database** command in privileged EXEC mode.

show crypto engine accelerator sa-database

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(1)XC	This command was introduced on the Cisco 1720 and Cisco 1750 platforms.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use this command when encrypted traffic is sent to the router and a problem with the encryption module is suspected.

Note The **show crypto engine accelerator sa-database** command is intended only for Cisco Systems TAC personnel to collect debugging information.

Examples

The following is sample output for the **show crypto engine accelerator sa-database** command:

```
Router# show crypto engine accelerator sa-database

Flow Summary
        Index   Algorithms
        005      tunnel inbound  esp-md5-hmac esp-des ah-sha-hmac
        006      tunnel outbound esp-md5-hmac esp-des ah-sha-hmac
        007      tunnel inbound  esp-md5-hmac esp-des ah-sha-hmac
        008      tunnel outbound esp-md5-hmac esp-des ah-sha-hmac
        009      tunnel inbound  esp-md5-hmac esp-des ah-sha-hmac
        010      tunnel outbound esp-md5-hmac esp-des ah-sha-hmac
SA Summary:
        Index   DH-Index        Algorithms
        003     001(deleted)    DES SHA
        004     002(deleted)    DES SHA
DH Summary
        Index Group Config
```

Related Commands

Command	Description
debug crypto engine acclerator logs	Enables logging of commands and associated parameters sent from the VPN module driver to the VPN module hardware using a debug flag.

show crypto engine accelerator statistic

To display IP Security (IPsec) encryption statistics and error counters for the onboard hardware accelerator of the router or the IPsec Virtual Private Network (VPN) Shared Port Adapter (SPA), use the **show crypto engine accelerator statistic** command in privileged EXEC mode.

show crypto engine accelerator statistic

IPsec VPN SPA (SPA-IPSEC-2G) and VSPA (WS-IPSEC-3G)

show crypto engine accelerator statistic [**slot** *slot*/*subslot* | **all**] [**coreutil** | **detail**]

Syntax Description

slot *slot*/*subslot*	(IPsec VPN SPA and VSPA only—Optional) Chassis slot number and secondary slot number on the SPA Interface Processor (SIP) where the SPA is installed. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide. Displays platform statistics for the corresponding SPA. This output will not include network interface controller statistics.
all	(IPsec VPN SPA and VSPA only—Optional) Displays platform statistics for all IPsec VPN SPAs or VSPAs on the router. This output will not include network interface controller statistics.
coreutil	(VSPA only—Optional) Displays VPN core utilization statistics.
detail	(IPsec VPN SPA and VSPA only—Optional) Displays platform statistics for the SPA and network interface controller statistics. Note that the controller statistics contain Layer 2 (L2) counters.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(1)XC	This command was introduced for the Cisco 1700 series router and other Cisco routers that support hardware accelerators for IPsec encryption.
12.1(3)XL	This command was implemented on the Cisco uBR905 cable access router.
12.2(2)XA	Support was added for the Cisco uBR925 cable access router.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented for the AIM-VPN/EPII and AIM-VPN/HPII on the following platforms: Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745. In addition, the output for this **show** command was enhanced to display compression statistics.
12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.

Release	Modification
12.3(4)T	The AIM-VPN/BPII was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA to support the IPsec VPN SPA on Cisco 7600 series routers.
12.4(9)T	Output was added for the AIM-VPN Secure Sockets Layer (SSL) encryption module.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH to support the IPsec VPN SPA on Catalyst 6500 series switches.
12.2(33)SXI	The **coreutil** keyword was added for the VSPA, and output was added to display the percent utilization with other utilization statistics in the crypto engine.
12.4(24)T	Output was modified to display reassembly and fragmentation-drop counters for VPN Service Adaptor (VSA) traffic statistics.

Usage Guidelines

No specific usage guidelines apply to the hardware accelerators.

IPsec VPN SPA and VSPA

Enter the **slot** keyword to display platform statistics for the corresponding SPA. This output will not include network interface controller statistics.

Enter the **all** keyword to display platform statistics for all IPsec VPN SPAs and VSPAs on the router. This output will not include network interface controller statistics.

Enter the **detail** keyword to display platform statistics for the SPA and network interface controller statistics. Note that the controller statistics contain L2 counters.

VSPA

Enter the **coreutil** keyword to display VPN core utilization statistics. This output will not include network interface controller statistics.

Tip In Cisco IOS Release 12.2(8)T and later releases, you can add a time stamp to show commands using the **exec prompt timestamp** command in line configuration mode.

Examples

Hardware VPN Module

The following example displays compression statistics for a hardware VPN module:

```
Router# show crypto engine accelerator statistic

Device:   AIM-VPN/SSL-3
Location: AIM Slot: 0
Virtual Private Network (VPN) Module in slot : 0
    Statistics for Hardware VPN Module since the last clear
     of counters 85319 seconds ago
               560 packets in                        560 packets out
             95600 bytes in                       124720 bytes out
                 0 paks/sec in                         0 paks/sec out
                 0 Kbits/sec in                        0 Kbits/sec out
```

```
                0 packets decrypted                   560 packets encrypted
                0 bytes before decrypt             124720 bytes encrypted
                0 bytes decrypted                   95600 bytes after encrypt
                0 packets decompressed                  0 packets compressed
                0 bytes before decomp                   0 bytes before comp
                0 bytes after decomp                    0 bytes after comp
                0 packets bypass decompr                0 packets bypass compres
                0 bytes bypass decompres                0 bytes bypass compressi
                0 packets not decompress                0 packets not compressed
                0 bytes not decompressed                0 bytes not compressed
                1.0:1 compression ratio                 1.0:1 overall
            10426 commands out                      10426 commands acknowledged
    Last 5 minutes:
                0 packets in                            0 packets out
                0 paks/sec in                           0 paks/sec out
                0 bits/sec in                           0 bits/sec out
                0 bytes decrypted                       0 bytes encrypted
                0 Kbits/sec decrypted                   0 Kbits/sec encrypted
                1.0:1 compression ratio                 1.0:1 overall

Errors:
   ppq full errors          :        0   ppq rx errors            :        0
   cmdq full errors         :        0   cmdq rx errors           :        0
   ppq down errors          :        0   cmdq down errors         :        0
   no buffer                :        0   replay errors            :        0
   dest overflow            :        0   authentication errors    :        0
   Other error              :        0   Raw Input Underrun       :        0
   IPSEC Unsupported Option:        0   IPV4 Header Length       :        0
   ESP Pad Length           :        0   IPSEC Decompression      :        0
   AH ESP seq mismatch      :        0   AH Header Length         :        0
   AH ICV Incorrect         :        0   IPCOMP CPI Mismatch      :        0
   IPSEC ESP Modulo         :        0   Unexpected IPV6 Extensio:        0
   Unexpected Protocol      :        0   Dest Buf overflow        :        0
   IPSEC Pkt is fragment    :        0   IPSEC Pkt src count      :        0
   Invalid IP Version       :        0   Unwrappable              :        0
   SSL Output overrun       :        0   SSL Decompress failure   :        0
   SSL BAD Decomp History   :        0   SSL Version Mismatch     :        0
   SSL Input overrun        :        0   SSL Conn Modulo          :        0
   SSL Input Underrun       :        0   SSL Connection closed    :        0
   SSL Unrecognised content:        0   SSL record header length:        0
   PPTP Duplicate packet    :        0   PPTP Exceed max missed p:        0
   RNG self test fail       :        0   DF Bit set               :        0
   Hash Miscompare          :        0   Unwrappable object       :        0
   Missing attribute        :        0   Invalid attrribute value:        0
   Bad Attribute            :        0   Verification Fail        :        0
   Decrypt Failure          :        0   Invalid Packet           :        0
   Invalid Key              :        0   Input Overrun            :        0
   Input Underrun           :        0   Output buffer overrun    :        0
   Bad handle value         :        0   Invalid parameter        :        0
   Bad function code        :        0   Out of handles           :        0
   Access denied            :        0   Out of memory            :        0
   NR overflow              :        0   pkts dropped             :        0

Warnings:
   sessions_expired         :        0   packets_fragmented       :        0
   general:                 :        0

HSP details:
   hsp_operations           :    10441   hsp_sessio
```

Table 86 describes significant fields shown in the above display.

Table 86 show crypto engine accelerator statistic Compression Statistics Descriptions

Counter	Description
packets decompressed	Number of packets that were decompressed by the interface.
packets compressed	Number of packets that were compressed by the interface.
bytes before decomp	Number of compressed bytes that were presented to the compression algorithm from the input interface on decrypt.
bytes before comp	Number of uncompressed bytes (payload) that were presented to the compression algorithm from Cisco IOS on encrypt.
bytes after decomp	Number of decompressed bytes that were sent to Cisco IOS by the compression algorithm on decryption.
bytes after comp	Number of compressed bytes that were forwarded to Cisco IOS by the algorithm on encryption.
packets bypass compres	Number of packets that were not compressed because they were too small (<128 bytes).
packets not compressed	Number of packets that were not compressed because the packets were expanded rather than compressed.
compression ratio	Ratio of compression and decompression of packets presented to the compression algorithm that were successfully compressed or decompressed. This statistic measures the efficiency of the algorithm for all packets that were compressed or decompressed.
overall	Ratio of compression and decompression of packets presented to the compression algorithm, including those that were not compressed due to expansion or too small. This ratio indicates whether the data traffic on this interface is suitable for compression. A ratio of 1:1 would imply that no successful compression is being performed on this data traffic.

7200/VSA

The following example is output from a Cisco 7200 with VSA:

```
Router# show crypto engine accelerator statistic 0
Inbound rate: 0pps 0kb/s  Outbound rate: 0pps 0kb/s

    TRAFFIC                     Transmitted                 Received
 ------------------------------------------------------------------------------
  Message  Count:                       5                        5
  Message  Byte Count:               1212                      256
  Message  Overflow:                    0
  Outbound Count:                      54                      154
  Outbound Byte Count:              12472                    30332
  Outbound Overflow:                    0
  Inbound  Count:                     153                      153
  Inbound  Byte Count:              26304                    19864
  Inbound  Overflow:                    0

  Reassembled Pkt:                      0
  Fragments Dropped:                    0
     IPPE:                              0
     EPPE:                              0
```

```
     FIFO:                                0
     RAE:                                 0

  Inbound Traffic:
 ------------------------------------------------------------------------------
  Decrypted Pkt:                       150
  Passthrough Pkt:                       3
  IKE Pkt:                               0

  SPI Error:                             0
  Policy Violation:                      0

  Outbound Traffic:            Route cache                 Processor
 ------------------------------------------------------------------------------
  Encrypted Pkt:                       150                         0
  Passthrough Pkt:                       0                         4
  Policy Violation:                      0

  Queue Depth:
 ------------------------------------------------------------------------------
  TXRing Current Queue Depth:
    High Priority   :                    0.0 %
    Medium Priority :                    0.0 %
    Low Priority    :                    0.0 %

VSA RX Exception statistics:
   Invalid SA              :          0   Enc Dec mismatch        :          0
   Next Header mismatch    :          0   Pad mismatch            :          0
   MAC mismatch            :          0   Anti replay failed      :          0
   Enc Seq num overflow    :          0   Dec IPver mismatch      :          0
   Enc IPver mismatch      :          0   TTL Decr                :          0
   Selector checks         :          0   UDP mismatch            :          0
   IP Parse error          :          0   Fragmentation Error     :          0
   IB Selector check       :          0   TimeBased Replay Err    :          0
   Misc. Exceptions        :          0
```

Table 87 describes significant fields shown in the above display.

Table 87 show crypto engine statistic Field Descriptions for a Cisco 7200/VSA

Field	Description
Message Count	Number of messages sent to the VSA.
Message Byte Count	Byte count for the above messages.
Message Overflow	Number of messages that could not be sent because there was no space in the transmission (TX) ring.
Outbound Count	Number of outbound packets sent to the VSA for classification and/or encryption (includes packets for encryption/passthrough).
Outbound Byte Count	Byte count of the above packets.
Outbound Overflow	Number of outbound packets that could not be sent.
Inbound Count	Number of inbound packets sent to the VSA for classification and/or decryption.
Inbound Byte Count	Byte count for the above packets.

Table 87 show crypto engine statistic Field Descriptions for a Cisco 7200/VSA (continued)

Field	Description
Inbound Overflow	Number of inbound packets that could not be sent because the TX ring was full.
Reassembled Pkt	Number of reassembled packets.
Fragments Dropped	Total number of fragments dropped.
IPPE	Number of inbound fragments dropped by the Ingress Packet Processing Engine (IPPE)
EPPE	Number of outbound fragments dropped by the Egress Packet Processing Engine (EPPE).
FIFO	Number of fragments dropped by the FIFO (First In First Out) fragment queue.
RAE	Number of fragments dropped by the Reassembly Engine (RAE).
Inbound Traffic	
Decrypted Pkt	Number of decrypted packets.
Passthrough Pkt	Clear packets in the inbound direction.
IKE Pkt	Internet Key Exchange (IKE) packets that were received.
SPI Error	Received packets having an invalid Security Parameter Index (SPI).
Policy Violation	The VSA received clear packets that should have come encrypted as per the policy.
Outbound Traffic	
Encrypted Pkt	Number of encrypted packets.
Passthrough Pkt	Outbound clear packets.
Policy Violation	No outbound SA to encrypt the packet.
Queue Depth	
TXRing Current Queue Depth	Current queue depth of the three TX rings.
VSA RX Exception statistics	Errors from the crypto chip.
Invalid SA	Specified SA does not exist.
Enc Dec mismatch	Packet came on the wrong type of SA.
Next Header mismatch	Wrong nextheader field was found in the packet.
Pad mismatch	Wrong pad found in the packet.
MAC mismatch	Authentication check failed.
Anti replay failed	Anti-replay error.
Enc Seq num overflow	Sequence number reached the max for the SA.
Dec IPver mismatch	Wrong IP version for the packet to be decrypted (for example, an IPv4 packet came in for an IPv6 SA).

Table 87 show crypto engine statistic Field Descriptions for a Cisco 7200/VSA (continued)

Field	Description
Enc IPver mismatch	Wrong IP version for the packet to be encrypted. Wrong IP version for the packet to be encrypted.
TTL Decr	Time to Live decremented to 0 (zero).
Selector checks	Decrypted packet failed the policy check.
UDP mismatch	User Data Protocol (UDP) packet failed the sanity check.
IP Parse error	Error in IP packet parsing.
Fragmentation Error	Could not fragment; DF bit set.
IB Selector check	Decrypted packet failed the policy check (for Group Encrypted Transport Virtual Private Network [GET VPN]).
TimeBased Replay Err	Time-based anti-replay failed (for GET VPN).
Misc. Exceptions	Errors not classified as any of the above.

IPsec VPN SPA and VSPA

The following example shows the platform statistics for the IPsec VPN SPA in slot 1 subslot 0 and also displays the network interface controller statistics (this platform output is from a Catalyst 6500 series with installed IPsec VPN SPA):

```
Router# show crypto engine accelerator statistic slot 1/0 detail

VPN module in slot 1/0


Decryption Side Data Path Statistics
====================================
Packets RX..............: 454260
Packets TX..............: 452480

IPSec Transport Mode.....: 0
IPSec Tunnel Mode........: 452470
AH Packets..............: 0
ESP Packets..............: 452470
GRE Decapsulations.......: 0
NAT-T Decapsulations.....: 0
Clear....................: 8
ICMP.....................: 0

Packets Drop.............: 193
Authentication Errors....: 0
Decryption Errors........: 0
Replay Check Failed......: 0
Policy Check Failed......: 0
Illegal CLear Packet.....: 0
GRE Errors...............: 0
SPD Errors...............: 0
HA Standby Drop..........: 0

Hard Life Drop...........: 0
Invalid SA...............: 191
SPI No Match.............: 0
Destination No Match.....: 0
```

```
Protocol No Match........: 0

Reassembly Frag RX.......: 0
IPSec Fragments..........: 0
IPSec Reasm Done.........: 0
Clear Fragments..........: 0
Clear Reasm Done.........: 0
Datagrams Drop...........: 0
Fragments Drop...........: 0


Decryption Side Controller Statistics

====================================
Frames RX................: 756088
Bytes RX.................: 63535848
Mcast/Bcast Frames RX....: 2341
RX Less 128Bytes.........: 756025
RX Less 512Bytes.........: 58
RX Less 1KBytes..........: 2
RX Less 9KBytes..........: 3
RX Frames Drop...........: 0

Frames TX................: 452365
Bytes TX.................: 38001544
Mcast/Bcast Frames TX....: 9
TX Less 128Bytes.........: 452343
TX Less 512Bytes.........: 22
TX Less 1KBytes..........: 0
TX Less 9KBytes..........: 0


Encryption Side Data Path Statistics
====================================
Packets RX...............: 756344
Packets TX...............: 753880
IPSec Transport Mode.....: 0
IPSec Tunnel Mode........: 753869
GRE Encapsulations.......: 0
NAT-T Encapsulations.....: 0
LAF prefragmented........: 0

Fragmented...............: 0
Clear....................: 753904
ICMP.....................: 0

Packets Drop.............: 123
IKE/TED Drop.............: 27
Authentication Errors....: 0
Encryption Errors........: 0
HA Standby Drop..........: 0

Hard Life Drop...........: 0
Invalid SA...............: 191

Reassembly Frag RX.......: 0
Clear Fragments..........: 0
Clear Reasm Done.........: 0
Datagrams Drop...........: 0
Fragments Drop...........: 0


Encryption Side Controller Statistics
====================================
```

```
Frames RX.................: 454065
Bytes RX..................: 6168274/
Mcast/Bcast Frames RX....: 1586
RX Less 128Bytes.........: 1562
RX Less 512Bytes.........: 452503
RX Less 1KBytes..........: 0
RX Less 9KBytes..........: 0
RX Frames Drop...........: 0

Frames TX.................: 753558
Bytes TX..................: 100977246
Mcast/Bcast Frames TX....: 2
TX Less 128Bytes.........: 3
TX Less 512Bytes.........: 753555
TX Less 1KBytes..........: 0
TX Less 9KBytes..........: 0
```

Table 88 describes significant fields shown in the above display.

Table 88 show crypto engine accelerator statistic IPsec VPN SPA Statistics Descriptions

Field	Description
Decryption Data Side Path Statistics	
Packets RX	Number of packets received on the decryption side of the IPsec VPN SPA.
Packets TX	Number of packets transmitted by the IPsec VPN SPA in the decryption direction.
IPSec Transport Mode	Number of packets in IPsec Transport Mode.
IPSec Tunnel Mode	Number of packets in IPsec Tunnel Mode.
AH Packets	Number of packets with authentication headers (AHs).
ESP Packets	Number of packets with Encapsulating Security Payload (ESP) headers.
GRE Decapsulations	Number of packets that were generic routing encapsulating (GRE) decapsulated.
NAT-T Decapsulations	Number of packets that were Network Address Translation-Traversal (NAT-T) decapsulated.
Clear	Number of clear packets received.
ICMP	Number of Internet Control Message Protocol (ICMP) packets received.
Packets Drop	Number of packet drops. **Note** Does not represent the sum of the individual drop subtotals displayed (does not include BPDU/CDP/MOP packets dropped).
Authentication Errors	Number of authentication errors.
Decryption Errors	Number of decryption errors.
Replay Check Failed	Number of replay check errors.

Table 88 show crypto engine accelerator statistic IPsec VPN SPA Statistics Descriptions (continued)

Field	Description
Policy Check Failed	Number of policy check errors.
Illegal Clear Packet	Number of illegal clear packets.
GRE Errors	Number of GRE errors due to invalid packets or invalid security associations (SAs). **Note** These errors correspond to the sum of the following GRE errors in the output of the **show stats icpu** command: "GRE Packet Errors," "GRE SA No Match," and "Invalid GRE SA," which count, respectively, the number of GRE packets that are RFC compliant but that use a format currently not supported by the VPN module, the number of GRE packets in which the SA lookup results is a no match, and the number of GRE packets in which the SA lookup matches an entry marked as invalid.
SPD Errors	Number of Security Policy Database (SPD) errors. **Note** These errors correspond to the sum of the following SPD errors in the output of the **show stats icpu** command: "SPD Lookup Failed," "SPD Invalid," and "SPD ID No Match."
HA Standby Drop	Number of packet drops on a High Availability (HA) standby IPsec VPN SPA. **Note** The standby IPsec VPN SA is not supposed to receive packets.
Hard Life Drop	Number of packet drops due to SA hard life expiration. **Note** These packets are dropped during rekeying after the SA volume lifetime has been reached.
Invalid SA	Number of packet drops due to invalid SA.
SPI No Match	Number of packet drops due to a Security Parameter Index (SPI) mismatch.
Destination No Match	Number of packet drops due to destination no match.
Protocol No Match	Number of packet drops due to protocol no match.
Reassembly Frag RX	Number of packets that required reassembly processing.
IPSec Fragments	Number of IPsec fragments.

Table 88 show crypto engine accelerator statistic IPsec VPN SPA Statistics Descriptions (continued)

Field	Description
IPSec Reasm Done	Number of IPsec fragments reassembled.
Clear Fragments	Number of clear fragments.
Clear Reasm Done	Number of clear fragments reassembled.
Datagrams Drop	Number of reassembled datagrams dropped.
Fragments Drop	Number of fragments dropped.
Decryption Side Controller Statistics	
Frames RX	Number of frames received.
Bytes RX	Number of bytes received.
Mcast/Bcast Frames RX	Number of multicast/broadcast frames received.
RX Less 128Bytes	Number of frames having a size less than 128 bytes.
RX Less 512Bytes	Number of frames having a size greater than or equal to 128 bytes and less than 512 bytes.
RX Less 1KBytes	Number of frames having a size greater than or equal to 512 bytes and less than 1 kilobyte (KB).
RX Less 9KBytes	Number of frames having a size greater than or equal to 1 KB and less than 9 KBs.
RX Frames Drop	Number of frames dropped.
Frames TX	Number of frames transmitted.
Bytes TX	Number of bytes transmitted.
Mcast/Bcast Frames TX	Number of multicast/broadcast frames transmitted.
TX Less 128Bytes	Number of frames having a size less than 128 bytes.
TX Less 512Bytes	Number of frames having a size greater than or equal to 128 bytes and less than 512 bytes.
TX Less 1KBytes	Number of frames having a size greater than or equal to 512 bytes and less than 1 KB.
TX Less 9KBytes	Number of frames having a size greater than or equal to 1 KB and less than 9 KBs.
Encryption Side Data Path Statistics	
Packets RX	Number of packets received on the encryption side of the IPsec VPN SPA.
Packets TX	Number of packets transmitted by the IPsec VPN SPA in the encryption direction.
IPSec Transport Mode	Number of packets in IPsec Transport Mode.
IPSec Tunnel Mode	Number of packets in IPsec Tunnel Mode.
GRE Encapsulations	Number of packets that were GRE encapsulated.

Table 88 show crypto engine accelerator statistic IPsec VPN SPA Statistics Descriptions (continued)

Field	Description
NAT-T Encapsulations	Number of packets that were NAT-T encapsulated.
LAF prefragmented	Number of packets with Look Ahead Fragmentation set and that were prefragmented.
Fragmented	Number of packets fragmented.
Clear	Number of clear packets.
ICMP	Number of ICMP packets.
Packets Drop	Number of packet drops. **Note** Does not represent the sum of the individual drop subtotals displayed (does not include BPDU/CDP/MOP packets dropped).
IKE/TED Drop	Number of packet drops because SA has not been set up.
Authentication Errors	Number of authentication errors.
Encryption Errors	Number of Encryption errors.
HA Standby Drop	Number of packet drops on a HA standby IPsec VPN SPA. **Note** The standby IPsec VPN SPA is not supposed to receive packets.
Hard Life Drop	Number of packet drops due to SA hard-life expiration. **Note** These packets are dropped during rekeying after the SA volume lifetime has been reached.
Invalid SA	Number of packet drops due to invalid SA.
Reassembly Frag RX	Number of packets that required reassembly processing.
Clear Fragments	Number of clear fragments.
Clear Reasm Done	Number of clear fragments reassembled.
Datagrams Drop	Number of reassembled datagrams dropped.
Fragments Drop	Number of fragments dropped.
Encryption Side Controller Statistics	
Frames RX	Number of frames received.
Bytes RX	Number of bytes received.
Mcast/Bcast Frames RX	Number of multicast/broadcast frames received.
RX Less 128Bytes	Number of frames having a size less than 128 bytes.

Table 88 show crypto engine accelerator statistic IPsec VPN SPA Statistics Descriptions (continued)

Field	Description
RX Less 512Bytes	Number of frames having a size greater than or equal to 128 bytes and less than 512 bytes.
RX Less 1KBytes	Number of frames having a size greater than or equal to 512 bytes and less than 1 KB.
RX Less 9KBytes	Number of frames having a size greater than or equal to 1 KB and less than 9 KBs.
RX Frames Drop	Number of frames dropped.
Frames TX	Number of frames transmitted.
Bytes TX	Number of bytes transmitted.
Mcast/Bcast Frames TX	Number of multicast/broadcast frames transmitted.
TX Less 128Bytes	Number of frames having a size less than 128 bytes.
TX Less 512Bytes	Number of frames having a size greater than or equal to 128 bytes and less than 512 bytes.
TX Less 1KBytes	Number of frames having a size greater than or equal to 512 bytes and less than 1 KB.
TX Less 9KBytes	Number of frames having a size greater than or equal to 1 KB and less than 9 KBs.

VSPA

The following examples show the output when the **coreutil** keyword is used with the VSPA and the Catalyst 6500 series switch using Cisco IOS Release 12.2(33)SXI and later releases:

```
Router#: show crypto engine accelerator statistic slot 2/0 coreutil

Utilization Percentages for VPN blade in slot 2/0
Blade Utilization Percentages
=========================
Last 5 seconds --------------------
Slowpath ..................... 35 %
Inbound ...................... 24 %
Outbound ..................... 32 %
QoS .......................... 44 %
Last 1 minute ----------------------
Slowpath ..................... 12 %
Inbound ...................... 11 %
Outbound ..................... 15 %
QoS .......................... 23 %
Last 5 minutes ---------------------
Slowpath ...................... 8 %
Inbound ...................... 11 %
Outbound ..................... 11 %
QoS .......................... 10 %

Router# show crypto engine accelerator statistic all coreutil

Utilization Percentages for VPN blade in slot 2/0
Blade Utilization Percentages
```

```
==========================
Last 5 seconds ---------------------
Slowpath ..................... 35 %
Inbound ...................... 24 %
Outbound ..................... 32 %
QoS .......................... 44 %
Last 1 minute ----------------------
Slowpath ..................... 12 %
Inbound ...................... 11 %
Outbound ..................... 15 %
QoS .......................... 23 %
Last 5 minutes ---------------------
Slowpath ...................... 8 %
Inbound ...................... 11 %
Outbound ..................... 11 %
QoS .......................... 10 %
Utilization Percentages for VPN blade in slot 2/1
Blade Utilization Percentages
==========================
Last 5 seconds ---------------------
Slowpath ..................... 88 %
Inbound ...................... 78 %
Outbound ..................... 79 %
QoS .......................... 32 %
Last 1 minute ----------------------
Slowpath ..................... 76 %
Inbound ...................... 80 %
Outbound ..................... 80 %
QoS .......................... 13 %
Last 5 minutes ---------------------
Slowpath ..................... 75 %
Inbound ...................... 65 %
Outbound ..................... 70 %
QoS .......................... 12 %
```

Table 89 describes significant fields shown in the above display.

Table 89 show crypto engine accelerator statistic coreutil VSPA Statistics Descriptions

Field	Description
Blade Utilization Percentages	
Slowpath	Utilization of slowpath traffic capacity.
Inbound	Utilization of inbound traffic capacity.
Outbound	Utilization of outbound traffic capacity.
QoS	Utilization of QoS traffic capacity.

Related Commands

Command	Description
clear crypto engine accelerator counter	Resets the statistical and error counters for the hardware accelerator to zero.
crypto ca	Defines the parameters for the certification authority used for a session.
crypto cisco	Defines the encryption algorithms and other parameters for a session.
crypto dynamic-map	Creates a dynamic map crypto configuration for a session.

Command	Description
crypto engine accelerator	Enables the use of the onboard hardware accelerator of the Cisco uBR905 and Cisco uBR925 routers for IPsec encryption.
crypto ipsec	Defines the IPsec SAs and transformation sets.
crypto isakmp	Enables and defines the IKE protocol and its parameters.
crypto key	Generates and exchanges keys for a cryptographic session.
crypto map	Creates and modifies a crypto map for a session.
debug crypto engine accelerator control	Displays each control command as it is given to the crypto engine.
debug crypto engine accelerator packet	Displays information about each packet sent for encryption and decryption.
show crypto engine accelerator ring	Displays the contents of command and transmit rings for the crypto engine.
show crypto engine accelerator sa-database	Displays the active (in-use) entries in the crypto engine security association (SA) database.
show crypto engine brief	Displays a summary of the configuration information for the crypto engine.
show crypto engine configuration	Displays the version and configuration information for the crypto engine.
show crypto engine connections	Displays a list of the current connections maintained by the crypto engine.

show crypto gdoi

To display information about a Group Domain of Interpretation (GDOI) configuration, use the **show crypto gdoi** command in privileged EXEC mode.

show crypto gdoi [**debug-condition**] [**group** *group-name*] [**gm** [**acl** | **rekey** | **replay**] | **ks** [**acl** | **coop** [**version**] | **members** [*ip-address*] | **policy** | **rekey** | **replay**]] [**ipsec sa**]

Syntax Description

debug-condition	(Optional) Displays GDOI debug conditional filters.
group *group-name*	(Optional) Displays information about the group specified.
gm	(Optional) Displays information about group members.
acl	(Optional) Displays the access control list (ACL) that has been applied to the GDOI group.
rekey	(Optional) Displays rekey information.
replay	(Optional) Displays group information for time-based anti-replay.
ks	(Optional) Displays information about key servers.
coop	(Optional) Displays information about the cooperative key servers.
version	(Optional) Displays information about the cooperative key server and client versions.
members [*ip-address*]	(Optional) Displays information about registered group members.
policy	(Optional) Displays key server policy information.
ipsec sa	(Optional) Displays information about the IP security (IPsec) security association (SA) for all group members. • If this keyword is used with the **group** *group-name* keyword and argument option, information is displayed for only the group that is specified.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(11)T	The **group** *group-name* keyword and argument and **gm**, **acl**, **rekey**, **replay**, **ks**, **coop** [**version**], **members**, **policy**, and **ipsec sa** keywords were added.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.
15.1(3)T	This command was modified. The **debug-condition** keyword was added.

Usage Guidelines

Because the **show running-config** command does not display enabled debug commands, the **debug-condition** keyword is useful for displaying GDOI debug conditional filters that are enabled.

Examples

The following output displays information about a configuration for a GDOI group member:

```
Router# show crypto gdoi group diffint

Group Information
   Group Name                  : diffint
   Group Identity              : 3333
   Group Members Registered    : 0
   Group Server                : 10.0.5.2


   Group Name                  : test
   Group Identity              : 4444
   Group Members Registered    : 0
   Group Server                : 10.0.5.2
```

The following output displays information about a configuration when entered on a GDOI key server:

```
Router# show crypto gdoi group diffint ks

Group Information
   Group Name                  : diffint
   Group Identity              : 3333
   Group Members Registered    : 1
   Group Server                : Local
   Group Rekey Lifetime        : 300 secs
   Group Rekey
       Remaining Lifetime      : 84 secs
   IPSec SA Number             : 1
     IPSec SA Rekey Lifetime   : 120 secs
     Profile Name              : gdoi-p
   SA Rekey
       Remaining Lifetime      : 64 secs
   access-list 120 permit ip host 10.0.1.1 host 192.168.1.1
   access-list 120 permit ip host 10.0.100.2 host 192.168.1.1

   Group Member List for Group diffint :
   Member ID                   : 10.0.3.1

   Group Name                  : test
   Group Identity              : 4444
   Group Members Registered    : 0
   Group Server                : Local
   Group Rekey Lifetime        : 600 secs
   IPSec SA Number             : 1
     IPSec SA Rekey Lifetime   : 120 secs
     Profile Name              : gdoi-p
   access-list 120 permit ip host 10.0.1.1 host 192.168.1.1
   access-list 120 permit ip host 10.0.100.2 host 192.168.1.1
```

The following output displays GDOI key server information for registered GMs when entered on a GDOI key server:

```
Router# show crypto gdoi ks members

Group Member Information :

Detail :

Number of rekeys sent for group diffint : 10

Group Member ID   : 5.0.6.1
Group ID          : 3333
Group Name        : diffint
```

```
Key Server ID     : 5.0.10.1
Rekeys sent       : 10
Rekeys retries    : 0
Rekey Acks Rcvd   : 10
Rekey Acks missed : 0

Sent seq num :    2    3    1    2
Rcvd seq num :    2    3    1    2

Group Member ID   : 5.0.5.1
Group ID          : 3333
Group Name        : diffint
Key Server ID     : 5.0.8.1
Rekeys sent       : 10
Rekeys retries    : 0
Rekey Acks Rcvd   : 10
Rekey Acks missed : 0

Sent seq num :    2    3    1    2
Rcvd seq num :    2    0    0    0
```

show crypto ha

To display all virtual IP (VIP) addresses that are currently in use by IP Security (IPSec) and Internet Key Exchange (IKE), use the **show crypto ha** command in privileged EXEC mode.

show crypto ha

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(11)T	This command was introduced.

Examples

The following output from the **show crypto ha** command shows all VIP addresses that are being used by IPSec and IKE:

```
Router# show crypto ha

IKE VIP: 209.165.201.3
  stamp: 74 BA 70 27 9C 4F 7F 81 3A 70 13 C9 65 22 E7 76
IKE VIP: 255.255.255.253
  stamp: Not set
IKE VIP: 255.255.255.254
  stamp: Not set
IPSec VIP: 209.165.201.3
IPSec VIP: 255.255.255.253
IPSec VIP: 255.255.255.254
```

show crypto identity

To display the crypto identity list, use the **show crypto identity** command in privileged EXEC mode.

show crypto identity [*identity-tag*]

Syntax Description

identity-tag	(Optional) The crypto identity tag value for which to display specific crypto identity list information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced in a release earlier than Cisco IOS Release 12.2(33)SRB.
12.2SX	This command was integrated into Cisco IOS Release 12.2SX.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
Cisco IOS XE 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Usage Guidelines

Use the **show crypto identity** command to display the configured crypto identity of a router.

Examples

The following are sample outputs from the **show crypto identity** command:

```
Router# show crypto identity id12

crypto identity id12:
   Description: line 22

Router# show crypto identity id11

crypto identity id11:
   fqdn line22

Router# show crypto identity

crypto identity tag12:
   Description: Linedescription
   fqdn fullyauthorisedone
```

Table 90 describes the significant fields shown in the display.

Table 90 show crypto identity Field Descriptions

Field	Description
Description	Line description.
fqdn	Fully qualified distinguished name identifier

show crypto ikev2 diagnose error

To display the current Internet Key Exchange Version 2 (IKEv2) exit path database, use the **show crypto ikev2 diagnose error** command in privileged EXEC mode.

show crypto ikev2 diagnose error [**count**]

Syntax Description

count	(Optional) Display the error counters from the exit path database.

Command Default

The IKEv2 exit path database is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to display the IKEv2 exit path database. Enable or disable IKEv2 exit path logging using the **crypto ikev2 diagnose error** command. Use the **clear crypto ikev2 diagnose error** command to clear the IKEv2 exit path database.

Examples

The following example is a sample output from the **show crypto ikev2 diagnose error** command. The output is self-explanatory.

```
Router# show crypto ikev2 diagnose error
Exit Path Table - status: enable, current entry 2, deleted 0, max allow 50

Error(1): No pskey found
 -Traceback= 0x37ABEB8z 0x37AC29Cz 0x2C0CA74z 0x2C0CA70z

Error(1): No pskey found
 -Traceback= 0x37B609Cz 0x37ABEB8z 0x37AC29Cz 0x2C0CA74z 0x2C0CA70z
```

Related Commands

Command	Description
clear crypto ikev2 diagnose error	Clears the IKEv2 exit path database.
crypto ikev2 diagnose error	Enables IKEv2 error diagnosis.

show crypto ikev2 policy

To display the default or a user-defined Internet Key Exchange Version 2 (IKEv2) policy, use the **show crypto ikev2 policy** command in privileged EXEC mode.

show crypto ikev2 policy [*policy-name*]

Syntax Description

policy-name	(Optional) Displays the specified policy.

Command Default

If no option is specified, then this command displays all the policies.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. The command output was updated to support IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to display the default or user-defined IKEv2 policy. User-defined policies display the default values of the commands that are not explicitly configured under the policy.

Examples

The following examples show the output for a default and user-defined policy.

Default IKEv2 Policy

The default IKEv2 policy matches all local addresses in global VRF and uses the default IKEv2 proposal.

```
Router# show crypto ikev2 policy default

 IKEv2 policy : default
      Match fvrf  : global
      Match address local : any
      Proposal    : default

Router# show crypto ikev2 policy default
```

This sample output shows the default IKEv2 policy that matches the local IPv6 address in global VRF:
IKEv2 policy : default

```
      Match fvrf  : global
      Match address local : 2001:DB8:1::1
      Proposal    : default
```

User-defined IKEv2 policy

```
Router# show crypto ikev2 policy policy-1

    IKEv2 policy : policy-1
        Match fvrf : green
        Match local : 10.0.0.1
        Proposal    : proposal-A
        Proposal    : proposal-B
```

Table 91 describes the significant fields shown in the display.

Table 91 show crypto ikev2 policy Field Descriptions

Field	Description
IKEv2 policy	Name of the IKEv2 policy.
Match fvrf	The front door virtual routing and forwarding (FVRF) specified for matching the IKEv2 policy.
Match local	The local IP address (IPv4 or IPv6) assigned for matching the IKEv2 policy.
Proposal	The name of the proposal that is attached to the IKEv2 policy.

Related Commands

Command	Description
crypto ikev2 policy	Defines an IKEv2 policy.
crypto ikev2 proposal	Defines an IKE proposal.
match (ikev2 policy)	Matches an IKEv2 policy based on the parameters.
proposal	Specifies the proposals that must be used in the IKEv2 policy.

show crypto ikev2 profile

To display a user-defined Internet Key Exchange Version 2 (IKEv2) profile, use the **show crypto ikev2 profile** command in privileged EXEC mode.

show crypto ikev2 profile [*profile-name*]

Syntax Description

profile-name	(Optional) Name of the IKEv2 profile.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. The command output was updated to support IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to display information about an IKEv2 profile. This command also displays the default values of the commands that are not explicitly configured in the IKEv2 profile. If a profile name is not specified, the command displays all the user-defined IKEv2 profiles.

Examples

The following example is sample output from the **show crypto ikev2 profile** command:

```
Router# show crypto ikev2 profile

IKEv2 profile: prof
 Ref Count: 3
 Match criteria:
  Fvrf: any
  Local address/interface: none
  Identities:
   fqdn smap-initiator
  Certificate maps: none
 Local identity: fqdn dmap-responder
 Remote identity: none
 Local authentication method: pre-share
 Remote authentication method(s): pre-share
 Keyring: v2-kr1
 Trustpoint(s): none
 Lifetime: 86400 seconds
 DPD: disabled
 NAT-keepalive: disabled
 Ivrf: global
```

```
Virtual-template: none
Accounting mlist: none
```

Table 92 describes the significant fields shown in the display.

Table 92 show crypto ikev2 profile Field Descriptions

Field	Description
IKEv2 profile	Name of the IKEv2 profile.
Match	The match parameter in the profile.
Local Identity	The local identity type.
Local authentication method	The local authentication methods.
Remote authentication method	The remote authentication methods.
Keyring	The keyring specified in the profile.
Trustpoint	The trustpoints used in the Rivest, Shamir and Adleman (RSA) signature authentication method.
Lifetime	The lifetime of the IKEv2 profile.
DPD	The status of Dead Peer Detection (DPD).
Ivrf	The Inside VRF (IVRF) in the profile.
Virtual-template	The virtual template in the profile.

show crypto ikev2 proposal

To display the Internet Key Exchange Version 2 (IKEv2) proposal, use the **show crypto ikev2 proposal** command in privileged EXEC mode.

show crypto ikev2 proposal [*name* | *default*]

Syntax Description

name	(Optional) The user-defined proposal.
default	(Optional) The default proposal.

Command Default

If no option is specified, the default and user-defined proposals are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to display the user-defined and default proposals.

Examples

The following example is a sample output from the **show crypto ikev2 proposal** command:

```
Router# show crypto ikev2 proposal

 IKEv2 proposal: pr1
     Encryption : 3DES AES-CBC-192
     Integrity  : MD596
     PRF        : MD5
     DH Group   : DH_GROUP_768_MODP/Group 1 DH_GROUP_1536_MODP/Group 5
 IKEv2 proposal: default
     Encryption : AES-CBC-128 3DES
     Integrity  : SHA96 MD596
     PRF        : SHA1 MD5
     DH Group   : DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2
```

Table 93 describes the significant fields shown in the display.

Table 93 show crypto ikev2 proposal Field Descriptions

Field	Description
IKEv2 proposal	Name of the proposal.
Encryption	The encryption algorithm configured in the proposal.
Integrity	The integrity algorithm configured in the proposal.

Table 93 show crypto ikev2 proposal Field Descriptions (continued)

Field	Description
PRF	The Pseudo-Random Function in the proposal. This is the same as the integrity algorithm.
DH Group	The Diffie-Hellman groups configured in the proposal.

Related Commands

Command	Description
crypto ikev2 proposal	Defines an IKEv2 proposal.
encryption (ikev2 proposal)	Specifies the encryption algorithm in an IKEv2 proposal.
group (ikev2 proposal)	Specifies the DH groups in an IKEv2 proposal.
integrity (ikev2 proposal)	Specifies the integrity algorithm in an IKEv2 proposal.

show crypto ikev2 sa

To display the Internet Key Exchange Version 2 (IKEv2) security associations (SA), use the **show crypto ikev2 sa** command in privileged EXEC mode.

show crypto ikev2 sa {**local** *ip-address* | **remote** *ip-address* | **fvrf** *vrf-name*} [**detailed**]

Syntax Description

local *ip-address*	Displays the current IKEv2 security associations matching the local address.
remote *ip-address*	Displays the current IKEv2 security associations matching the remote address.
fvrf *vrf-name*	Displays the current IKEv2 security associations matching the specified front door virtual routing and forwarding (FVRF).
detailed	(Optional) Displays detailed information about the current security associations.

Command Default

All the current IKEv2 security associations are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to display information about the current IKEv2 security associations.

Examples

The following is sample output from the **show crypto ikev2 sa** command:

```
Router# show crypto ikev2 sa

Tunnel-id   Local          Remote           fvrf/ivrf          Status
2           10.0.0.1/500    10.0.0.2/500      (none)/(none)      READY
      Encr: 3DES, Hash: SHA96, DH Grp:2, Auth: PSK
      Life/Active Time: 86400/361 sec
```

The following is sample output from the **show crypto ikev2 sa detailed** command:

```
Router# show crypto ikev2 sa detailed

Tunnel-id Local                Remote                fvrf/ivrf            Status
1         1.1.1.1/500          1.1.1.2/500           (none)/(none)        READY
      Encr: 3DES, Hash: MD596, DH Grp:2, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/12 sec
      CE id: 1001, Session-id: 1
      Status Description: Negotiation done
      Local spi: 41E942F807BA4153       Remote spi: 993043F2AF648C48
```

```
Local id: 1.1.1.1
Remote id: 1.1.1.2
Local req msg id:  2              Remote req msg id:  0
Local next msg id: 2              Remote next msg id: 0
Local req queued:  2              Remote req queued:  0
Local window:      5              Remote window:      5
DPD configured for 0 seconds, retry 0
NAT-T is not detected
```

Table 94 describes the significant fields shown in the display.

Table 94 show crypto ikev2 sa detailed Field Descriptions

Field	Description
Tunnel-id	Unique identifier of the IKEv2 tunnel.
Local	IP address and UDP port of the local IKEv2 endpoint.
Remote	IP address and UDP port of the remote IKEv2 endpoint.
fvrf/ivrf	FVRF/IVRF of the local IKEv2 endpoint.
Status	Status of the IKEv2 tunnel.
Encr	Encryption algorithm used by the IKEv2 tunnel.
Hash	Integrity algorithm used by the IKEv2 tunnel.
DH Grp	Diffie-Hellman (DH) group used by the IKEv2 tunnel.
Auth Sign	Authentication method used by the local IKEv2 endpoint.
Auth Verify	Authentication method used by the remote IKEv2 endpoint.
Life/Active Time	The total and active lifetime of the IKEv2 tunnel.
CE id	The crypto engine ID used by the local IKEv2 endpoint.
Session-id	The session ID for the IKEv2 tunnel.
MIB-id	The MIB identifier for the IKEv2 tunnel.
Status Description	Description of the IKEv2 tunnel status.
Local spi	IKEv2 security parameter index (SPI) of the local IKEv2 endpoint.
Remote spi	IKEv2 SPI of the remote IKEv2 endpoint.
Local id	IKEv2 identity of the local IKEv2 endpoint
Remote id	IKEv2 identity of the remote IKEv2 endpoint.
Local req mess id	Message ID of the last IKEv2 request sent.
Remote req mess id	Message ID of the last IKEv2 request received.
Local next mess id	Message ID of the next IKEv2 request to be sent.
Remote next mess id	Message ID of the next IKEv2 request to be received.
Local req queued	Number of requests queued to be sent.
Remote req queued	Number of requests queued to be processed.
Local window	IKEv2 window size of the local IKEv2 endpoint.
Remote window	IKEv2 window size of the remote IKEv2 endpoint.

Table 94 show crypto ikev2 sa detailed Field Descriptions (continued)

Field	Description
DPD	DPD interval.
NAT-T	NAT detection status.

show crypto ikev2 session

To display the status of active Internet Key Exchange Version 2 (IKEv2) sessions, use the **show crypto ikev2 session** command in privileged EXEC mode.

show crypto ikev2 session [**detailed**]

Syntax Description

detailed	(Optional) Displays detailed information about the session.

Command Default

The session information is displayed in a brief format.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. The command output was updated to support IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to display information about the active IKEv2 sessions. Use the **detailed** keyword to display information about IKEv2 parent and child security associations.

Examples

The following is a sample output from the **show crypto ikev2 session** and **show crypto ikev2 session detailed** command.

```
Router# show crypto ikev2 session

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id   Local           Remote           fvrf/ivrf          Status
1           10.0.0.1/500     10.0.0.2/500      (none)/(none)      READY
      Encr: 3DES, Hash: SHA96, DH Grp:2, Auth: PSK
      Life/Active Time: 86400/65 sec
CHild sa: local selector  10.0.0.1/0 - 10.0.0.1/65535
          remote selector 10.0.0.2/0 - 10.0.0.2/65535
          ESP spi in/out: 0x9360A95/0x6C340600
          CPI in/out: 0x9FE5/0xC776

Router# show crypto ikev2 session detailed

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id   Local          Remote           fvrf/ivrf          Status
1           10.0.0.1/500    10.0.0.2/500      (none)/(none)      READY
      Encr: 3DES, Hash: SHA96, DH Grp:2, Auth: PSK
```

```
      Life/Remaining/Active Time: 86400/86157/248 sec
      CE id: 0, Session-id: 1, MIB-id: 1
      Status Description: Negotiation done
      Local spi: 750CBE827434A245       Remote spi: 4353FEDBABEBF24C
      Local id:          10.0.0.1        Remote id:          10.0.0.2
      Local req mess id:    0           Remote req mess id: 0
      Local next mess id:    0          Remote next mess id: 2
      Local req queued:    0            Remote req queued: 0
      Local window:    5                 Remote window: 5
      DPD configured for 0 seconds
      NAT-T is not detected
Child sa: local selector  10.0.0.1/0 - 10.0.0.1/65535
          remote selector 10.0.0.2/0 - 10.0.0.2/65535
          ESP spi in/out: 0x9360A95/0x6C340600
          CPI in/out: 0x9FE5/0xC776
          AH spi in/out: 0x0/0x0
          Encr: AES CBC, keysize: 128, esp_hmac: SHA96
          ah_hmac: Unknown - 0, comp: IPCOMP_LZS, mode tunnel
```

Table 95 describes the significant fields shown in the display.

Table 95 show crypto ikev2 session detailed Field Descriptions

Field	Description
Tunnel id	Unique identifier of IKEv2 tunnel.
Local	IP address (IPv4 or IPv6) and UDP port of the local IKEv2 endpoint.
Remote	IPv4 or IPv6 address and UDP port of the remote IKEv2 endpoint.
fvrf/ivrf	FVRF/IVRF of the local IKEv2 endpoint.
Status	Status of the IKEv2 tunnel.
Encr	Encryption algorithm used by the IKEv2 tunnel.
Hash	Integrity algorithm used by the IKEv2 tunnel.
DH Grp	DH group used by the IKEv2 tunnel.
Auth Sign	Authentication method used by the local IKEv2 endpoint.
Auth Verify	Authentication method used by the remote IKEv2 endpoint.
Life/Active Time	The total and active lifetime of the IKEv2 tunnel.
CE id	The crypto engine ID used by the local IKEv2 endpoint.
Session-id	The session ID for the IKEv2 tunnel.
MIB-id	The MIB identifier for the IKEv2 tunnel.
Status Description	Description of the IKEv2 tunnel status.
Local spi	IKEv2 security parameter index (SPI) of the local IKEv2 endpoint.
Remote spi	IKEv2 SPI of the remote IKEv2 endpoint.
Local id	IKEv2 identity of the local IKEv2 endpoint
Remote id	IKEv2 identity of the remote IKEv2 endpoint.
Local req mess id	Message ID of the last IKEv2 request sent.
Remote req mess id	Message ID of the last IKEv2 request received.

Table 95 show crypto ikev2 session detailed Field Descriptions (continued)

Field	Description
Local next mess id	Message ID of the next IKEv2 request to be sent.
Remote next mess id	Message ID of the next IKEv2 request to be received.
Local req queued	Number of requests queued to be sent.
Remote req queued	Number of requests queued to be processed.
Local window	IKEv2 window size of the local IKEv2 endpoint.
Remote window	IKEv2 window size of the remote IKEv2 endpoint.
DPD	DPD interval.
NAT	NAT detection status.
Child sa: local selector	Local network protected by the child security association (SA).
remote selector	Remote network protected by the child SA.
ESP spi in/out	Inbound and outbound SPI of the Encapsulating Security Payload (ESP) child SA.
CPI in/out	Inbound and outbound Cisco Product Identification (CPI) of the IP compression (IPComp) child SA.
AH spi in/out	Inbound and outbound SPI of the Authentication Header (AH) child SA.
Encr	Encryption algorithm used by the ESP child SA.
keysize	Size of the key in bits used by the encryption algorithm.
esp_hmac	Integrity algorithm used by the ESP child SA.
ah_hmac	Integrity algorithm used in the AH child SA, if available.
comp	Compression algorithm used by IPComp child SA.
mode	Tunnel or transport mode used by ESP/AH child SA.

show crypto ikev2 stats

To display the Internet Key Exchange Version 2 (IKEv2) security associations (SAs) statistics, use the **show crypto ikev2 stats** command in privileged EXEC mode.

show crypto ikev2 stats

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to display IKEv2 security associations statistics.

Examples

The following example is a sample output from the **show crypto ikev2 stats** command. The fields in the output are self-explanatory.

```
Router(#) show crypto ikev2 stats
------------------------------------------------------------------------
              Crypto IKEV2 SA Statistics
------------------------------------------------------------------------
System Resource Limit:   0        Max IKEv2 SAs: 0        Max in nego: 1000
Total IKEv2 SA Count:    1        active:        1        negotiating: 0
Incoming IKEv2 Requests: 0        accepted:      0        rejected:    0
Outgoing IKEv2 Requests: 1        accepted:      1        rejected:    0
Rejected IKEv2 Requests: 0        rsrc low:      0        SA limit:    0
IKEv2 packets dropped at dispatch: 0
Incoming IKEV2 Cookie Challenged Requests: 0
    accepted: 0        rejected: 0        rejected no cookie: 0
```

show crypto ipsec client ezvpn

To display the Cisco Easy VPN Remote configuration, use the **show crypto ipsec client ezvpn** command in privileged EXEC mode.

show crypto ipsec client ezvpn

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(4)YA	This command was introduced on Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Examples

The following example shows a typical display from the **show crypto ipsec client ezvpn** command for an active Virtual Private Network (VPN) connection when the router is in client mode. The last two lines indicate that a configuration URL and configuration version number have been pushed through the Mode-Configuration Exchange by the server to the Easy VPN remote device.

```
Router# show crypto ipsec client ezvpn

Tunnel name: hw1
Inside interface list: FastEthernet0/0, Serial1/0,
Outside interface: Serial0/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 192.168.201.0
Mask: 255.255.255.224
DNS Primary: 192.168.201.1
DNS Secondary: 192.168.201.2
NBMS/WINS Primary: 192.168.201.3
NBMS/WINS Secondary: 192.168.201.4
Default Domain: cisco.com
Configuration URL: http://10.8.8.88/easy.cfg
Configuration Version: 10
```

The following example shows a typical display from the **show crypto ipsec client ezvpn** command for an active VPN connection when the router is in network-extension mode:

```
Router# show crypto ipsec client ezvpn

Tunnel name: hw1
Inside interface list: FastEthernet0/0, Serial1/0,
```

```
Outside interface: Serial0/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 192.168.202.128
Mask: 255.255.255.224
Default Domain: cisco.com

Split Tunnel List: 1
       Address    : 192.168.200.225
       Mask       : 255.255.255.224
       Protocol   : 0x0
       Source Port: 0
       Dest Port  : 0
```

The following example shows a typical display from the **show crypto ipsec client ezvpn** command for an inactive VPN connection:

```
Router# show crypto ipsec client ezvpn

Current State: IDLE
Last Event: REMOVE INTERFACE CFG
Router#
```

The following example displays information about the outside interface “Virtual-Access1”, which is bound to the real interface (Ethernet0/0) on which the user has configured Easy VPN as an outside interface:

```
Router# show crypto ipsec client ezvpn

Easy VPN Remote Phase: 5
Tunnel name : ez
Inside interface list: Ethernet1/0,
Outside interface: Virtual-Access1 (bound to Ethernet0/0)
Easy VPN connect ACL checking active
Connect : ACL based with access-list 101
Current State: CONNECT_REQUIRED
Last Event: TRACKED OBJECT UP
Save Password: Disallowed
Current EzVPN Peer: 10.0.0.2
```

Table 96 describes significant fields shown by the **show crypto ipsec client ezvpn** command:

Table 96 show crypto ipsec client ezvpn Field Descriptions

Field	Description
Current State	Displays whether the VPN tunnel connection is active or idle. Typically, when the tunnel is up, the current state is IPSEC ACTIVE.
Last Event	Displays the last event performed on the VPN tunnel. Typically, the last event before a tunnel is created is SOCKET UP.
Address	Displays the IP address used on the outside interface.
Mask	Displays the subnet mask used for the outside interface.
DNS Primary	Displays the primary domain name system (DNS) server provided by the Dynamic Host Configuration Protocol (DHCP) server.
DNS Secondary	Displays the secondary DNS server provided by the DHCP server.
Domain Name	Displays the domain name provided by the DHCP server.

Table 96 show crypto ipsec client ezvpn Field Descriptions (continued)

Field	Description
NBMS/WINS Primary	Displays the primary NetBIOS Microsoft Windows Name Server provided by the DHCP server.
NBMS/WINS Secondary	Displays the secondary NetBIOS Microsoft Windows Name Server provided by the DHCP server.

Related Commands

Command	Description
show crypto ipsec transform	Displays the specific configuration for one or all transformation sets.

show crypto ipsec default transform-set

To display the default IP Security (IPsec) transform sets currently in use by Internet Key Exchange (IKE), use the **show crypto ipsec default transform-set** command in privileged EXEC mode.

show crypto ipsec default transform-set

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

If the default transform sets are in use, the **show crypto ipsec default transform-set** command displays the two default transform sets each of which defines an Encapsulation Security Protocol (ESP) encryption transform type and an ESP authentication transform type.

Examples

The following example displays the two default transform sets. No user defined transform sets have been configured, the default transform sets have not been disabled, and the crypto engine supports the encryption algorithm.

```
Router# show crypto ipsec default transform-set

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
```

Table 97 show crypto ipsec default transform-set Field Descriptions

Default Transform Name	ESP Encryption Transform and Description	ESP Authentication Transform and Description
#$!default_transform_set_1	esp-aes (ESP with the 128-bit Advanced Encryption Standard [AES] encryption algorithm)	esp-sha-hmac (ESP with the Secure Hash Algorithm [SHA-1, HMAC variant] authentication algorithm)
#$!default_transform_set_0	esp-3des (ESP with the 168-bit Triple Data Encryption Standard [3DES or Triple DES] encryption algorithm)	esp-sha-hmac

The following example shows that when the default transform sets are disabled with the **no crypto ipsec default transform-set**, the **show crypto ipsec default transform-set** has no output.

```
Router(config)# no crypto ipsec default transform-set
Router(config)# exit
Router#
Router# show crypto ipsec default transform-set

Router#
```

Related Commands

Command	Description
crypto ipsec transform-set	Defines a transform set.
show crypto ipsec transform-set	Displays the configured transform sets.
show crypto map (IPsec)	Displays the crypto map configuration.

show crypto ipsec sa

To display the settings used by current security associations (SAs), use the **show crypto ipsec sa** command in privileged EXEC mode.

show crypto ipsec sa [**map** *map-name* | **address** | **identity** | **interface** *type number* | **peer** [**vrf** *fvrf-name*] **address** | **vrf** *ivrf-name* | **ipv6** [**interface** *type number*]] [**detail**]

IPsec and IKE Stateful Failover Syntax

show crypto ipsec sa [**active** | **standby**]

Syntax Description

map *map-name*	(Optional) Displays any existing SAs that were created for the crypto map set with the value for the *map-name* argument.
address	(Optional) Displays all existing SAs, sorted by the destination address (either the local address or the address of the IP security (IPsec) remote peer) and then by protocol (Authentication Header [AH] or Encapsulation Security Protocol [ESP]).
identity	(Optional) Displays only the flow information. SA information is not shown.
interface *type number*	(Optional) Displays all existing SAs created for the interface value provided in the *interface* argument.
peer [**vrf** *fvrf-name*] **address**	(Optional) Displays all existing SAs with the peer address. If the peer address is in the Virtual Routing and Forwarding (VRF), specify **vrf** and the *fvrf-name*.
vrf *ivrf-name*	(Optional) Displays all existing SAs whose inside virtual routing and forwarding (IVRF) is the same as the valued used for the *ivrf-name* argument.
ipv6	(Optional) Displays IPv6 crypto IPsec SAs.
detail	(Optional) Detailed error counters. (The default is the high-level send or receive error counters.)
active	(Optional) Displays high availability (HA) - enabled IPsec SAs that are in the active state.
standby	(Optional) Displays HA-enabled IPsec SAs that are in the standby state.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3T	This command was introduced.
12.2(13)T	The “remote crypto endpt” and “in use settings” fields were modified to support Network Address Translation (NAT) traversal.

Release	Modification
12.2(15)T	The **interface** keyword and *type* and *number* arguments were added. The **peer** keyword, the **vrf** keyword, and the *fvrf-name* argument were added. The **address** keyword was added to the **peer** keyword string. The **vrf** keyword and *ivrf-name* argument were added.
12.3(11)T	The **active** and **standby** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was modified. This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

If no keyword is used, all SAs are displayed. They are sorted first by interface and then by traffic flow (for example, source or destination address, mask, protocol, or port). Within a flow, the SAs are listed by protocol (ESP or AH) and direction (inbound or outbound).

Examples

The following is sample output from the **show crypto ipsec sa** command:

```
Router# show crypto ipsec sa

interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 10.5.5.2
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.5.5.2/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (10.5.5.1/255.255.255.255/47/0)
   current_peer 10.5.5.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 492908510, #pkts encrypt: 492908510, #pkts digest: 492908510
    #pkts decaps: 492908408, #pkts decrypt: 492908408, #pkts verify: 492908408
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 55, #recv errors 0

     local crypto endpt.: 10.5.5.2, remote crypto endpt.: 10.5.5.1
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/2
     current outbound spi: 0xDE4EE29D(3729711773)

     inbound esp sas:
       spi: 0xC06CA92B(3228346667)
         transform: esp-3des esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 3139, flow_id: VSA:1139, crypto map: Tunnel1-head-0
         sa timing: remaining key lifetime (k/sec): (3948785/556)
         IV size: 8 bytes
         replay detection support: Y
         Status: ACTIVE

     inbound ah sas:
       spi: 0xC87AB936(3363486006)
         transform: ah-md5-hmac ,
         in use settings ={Tunnel, }
```

```
        conn id: 3139, flow_id: VSA:1139, crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (3948785/556)
        replay detection support: Y
        Status: ACTIVE

    inbound pcp sas:

    outbound esp sas:
      spi: 0xDE4EE29D(3729711773)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 3140, flow_id: VSA:1140, crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (3948785/556)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

    outbound ah sas:
      spi: 0xAEEDD4F1(2934822129)
        transform: ah-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 3140, flow_id: VSA:1140, crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (3948785/556)
        replay detection support: Y
        Status: ACTIVE

    outbound pcp sas:
```

The following is sample output from the **show crypto ipsec sa identity detail** command:

```
Router# show crypto ipsec sa identity detail

interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 10.5.5.2
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer (none) port 500
     DENY, flags={ident_is_root,}
     #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
     #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #pkts no sa (send) 0, #pkts invalid sa (rcv) 0
     #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
     #pkts invalid prot (recv) 0, #pkts verify failed: 0
     #pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
     #pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
     ##pkts replay failed (rcv): 0
     #pkts internal err (send): 0, #pkts internal err (recv) 0

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.5.5.2/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (10.5.5.1/255.255.255.255/47/0)
   current_peer 10.5.5.1 port 500
     PERMIT, flags={origin_is_acl,}
     #pkts encaps: 492923510, #pkts encrypt: 492923510, #pkts digest: 492923510
     #pkts decaps: 492923408, #pkts decrypt: 492923408, #pkts verify: 492923408
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #pkts no sa (send) 55, #pkts invalid sa (rcv) 0
     #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
```

```
#pkts invalid prot (recv) 0, #pkts verify failed: 0
#pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
##pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (recv) 0
```

Table 98 describes the significant fields shown in the above displays (**show crypto ipsec sa** and **show crypto ipsec sa detail**).

Table 98 show crypto ipsec sa Field Descriptions

Field	Description
crypto map tag	Policy tag for IPsec.
protected vrf	IVRF name that applies to the IPsec interface.
local ident (addr/mask/prot/port)	Local selector that is used for encryption and decryption.
remote ident (addr/mask/prot/port)	Remote selector that is used for encryption and decryption.
current peer	Current peer with which the IPsec tunnel communicates.
PERMIT, flags	IPsec SA is triggered by the Access Control List (ACL) permit action.
pkts encaps	Statistics number of packets that were successfully encapsulated by IPsec.
pkts encrypt	Statistics number of packets that were successfully encrypted by IPsec.
pkts digest	Statistics number of packets that were successfully hash digested by IPsec.
pkts decaps	Statistics number of packets that were successfully decapsulated by IPsec.
pkts decrypt	Statistics number of packets that were successfully decrypted by IPsec.
pkts verify	Received packets that passed the hash digest check.
pkts compressed	Number of packets that were successfully compressed by IPsec.
pkts decompressed	Number of packets that were successfully decompressed by IPsec.
pkts not compressed	Number of outbound packets that were not compressed.
pkts compr. failed	Number of packets that failed compression by IPsec.
pkts not decompressed	Number of inbound packets that were not compressed.
pkts decompress failed	Number of packets that failed decompression by IPsec.
send errors	Number of outbound packets that had errors.
recv errors	Number of inbound packets that had errors.
local crypto endpt.	Local endpoint terminated by IPsec.
remote crypto endpt.	Remote endpoint terminated by IPsec.

Table 98 show crypto ipsec sa Field Descriptions

Field	Description
path mtu	Maximum transmission unit (MTU) size that is figured based on the Internet Control Message Protocol (ICMP) unreachable packet. This value also has to consider the IPsec overhead.
ip mtu	Interface MTU size that considers the IPsec overhead.
current outbound spi	Current outbound Security Parameters Index (SPI).
ip mtu idb	Interface description block (IDB) that is used to determine the crypto IP MTU.
current outbound spi	Current outbound Security Parameter Index (SPI).
inbound esp sas	Encapsulating Security Payload (ESP) for the SA for the inbound traffic.
spi	SPI for classifying the inbound packet.
transform	Security algorithm that is used to provide authentication, integrity, and confidentiality.
in use settings	Transform that the SA uses (for example: tunnel mode, transport mode, UDP-encapsulated tunnel mode, or UDP-encapsulated transport mode).
conn id	ID that is stored in the crypto engine to identify the IPsec/Internet Key Exchange (IKE) SA.
flow_id	SA identity.
crypto map	Policy for the IPsec.
sa timing: remaining key lifetime (k/sec)	Seconds or kilobytes remaining before a rekey occurs.
IV size	Size of the initialization vector that is used for the cryptographic synchronization data used to encrypt the payload.
replay detection support	A specific SA has enabled the replay detection feature.
inbound ah sas	Authentication algorithm for the SA for inbound traffic.
inbound pcp sas	Compression algorithm for the SA for inbound traffic.
outbound esp sas	Encapsulating security payload for the SA for outbound traffic.
outbound ah sas	Authentication algorithm for the SA for outbound traffic.
outbound pcp sas	Compression algorithm for the SA for outbound traffic.
DENY, flags	IPsec SA is triggered by the ACL deny action.
pkts decompress failed	Number of packets decompressed by IPsec that failed.
pkts no sa (send)	Outbound packets cannot find the associated IPsec SA.
pkts invalid sa (rcv)	Received packets that failed the IPsec format check.
pkts invalid prot (recv)	Received packets that have the wrong protocol field.
pkts verify failed	Received packets that failed the hash digest check.

Table 98 show crypto ipsec sa Field Descriptions

Field	Description
pkts invalid identity (recv)	Packets after decryption cannot find the associated selector.
pkts pkts invalid len (rcv)	For the software crypto engine, inbound packets that have an incorrect pad length.
pkts replay rollover (send)	Sent packets that failed the replay test check.
pkts replay rollover (rcv)	Received packets that failed the replay test check.
pkts internal err (send)	Sent packets that failed because of a software or hardware error.
pkts internal err (rcv)	Received packets that failed because of a software or hardware error.
protected vrf	IVRF name that applies to the IPsec interface.

show crypto ipsec sa vrf Command Output

The following is sample output from the **show crypto ipsec sa vrf** command:

```
Router# show crypto ipsec sa vrf vpn2

interface: Ethernet1/2
    Crypto map tag: ra, local addr. 172.16.1.1

   protected vrf: vpn2
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (10.4.1.4/255.255.255.255/0/0)
   current_peer: 10.1.1.1:500
     PERMIT, flags={}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 172.16.1.1, remote crypto endpt.: 10.1.1.1
     path mtu 1500, media mtu 1500
     current outbound spi: 50110CF8

     inbound esp sas:
      spi: 0xA3E24AFD(2749516541)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5127, flow_id: 7, crypto map: ra
        sa timing: remaining key lifetime (k/sec): (4603517/3503)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x50110CF8(1343294712)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5128, flow_id: 8, crypto map: ra
```

```
        sa timing: remaining key lifetime (k/sec): (4603517/3502)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:
```

The following configuration was in effect when the preceding **show crypto ipsec sa vrf** command was issued. The IPsec remote access tunnel was "UP" when this command was issued.

```
crypto dynamic-map vpn1 1
 set transform-set vpn1
 set isakmp-profile vpn1-ra
 reverse-route
!
crypto dynamic-map vpn2 1
 set transform-set vpn2
 set isakmp-profile vpn2-ra
 reverse-route
!
!
crypto map ra 1 ipsec-isakmp dynamic vpn1
crypto map ra 2 ipsec-isakmp dynamic vpn2
```

Table 99 describes the significant fields shown in the preceding **show crypto ipsec sa vrf** display. Additional fields are self-explanatory or can be found in Table 98.

Table 99 show crypto ipsec sa vrf Field Descriptions

Field	Description
remote crypto endpt.	Remote endpoint terminated by IPsec.
media mtu	MTU value for media, such as an Ethernet or a serial interface.
inbound esp sas	Encapsulating security payload for the SA of the inbound traffic.

IPsec and IKE Stateful Failover Examples

The following sample output shows the IPsec SA status of only the active device:

```
Router# show crypto ipsec sa active

interface: Ethernet0/0
    Crypto map tag: to-peer-outside, local addr 10.165.201.3

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.0.1/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (172.16.0.1/255.255.255.255/0/0)
   current_peer 209.165.200.225 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 209.165.201.3, remote crypto endpt.: 209.165.200.225
     path mtu 1500, media mtu 1500
```

```
    current outbound spi: 0xD42904F0(3559458032)

    inbound esp sas:
     spi: 0xD3E9ABD0(3555306448)
       transform: esp-3des ,
       in use settings ={Tunnel, }
       conn id: 2006, flow_id: 6, crypto map: to-peer-outside
       sa timing: remaining key lifetime (k/sec): (4586265/3542)
            HA last key lifetime sent(k): (4586267)
       ike_cookies: 9263635C CA4B4E99 C14E908E 8EE2D79C
       IV size: 8 bytes
       replay detection support: Y
       Status: ACTIVE
```

Table 100 describes the significant fields shown in the preceding **show crypto ipsec sa active** display. Additional fields are self-explanatory or can be found in Table 98 or Table 99.

Table 100 show crypto ipsec sa active Field Descriptions.

Field	Description
HA last key lifetime sent (k)	Last stored kilobytes lifetime value for HA.
ike_cookies	ID that identifies the IKE SAs.

The following sample output shows the IPsec SA status of only the standby device. The fields in the display are either self-explanatory or can be found in Table 98, Table 99, or Table 100.

```
Router# show crypto ipsec sa standby

interface: Ethernet0/0
    Crypto map tag: to-peer-outside, local addr 10.165.201.3

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.0.1/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (172.16.0.1/255.255.255.255/0/0)
   current_peer 209.165.200.225 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 209.165.201.3, remote crypto endpt.: 209.165.200.225
     path mtu 1500, media mtu 1500
     current outbound spi: 0xD42904F0(3559458032)

     inbound esp sas:
      spi: 0xD3E9ABD0(3555306448)
        transform: esp-3des ,
        in use settings ={Tunnel, }
        conn id: 2012, flow_id: 12, crypto map: to-peer-outside
        sa timing: remaining key lifetime (k/sec): (4441561/3486)
             HA last key lifetime sent(k): (4441561)
        ike_cookies: 00000000 00000000 00000000 00000000
        IV size: 8 bytes
        replay detection support: Y
        Status: STANDBY

     inbound ah sas:
```

```
 spi: 0xF3EE3620(4092474912)
   transform: ah-md5-hmac ,
   in use settings ={Tunnel, }
   conn id: 2012, flow_id: 12, crypto map: to-peer-outside
   sa timing: remaining key lifetime (k/sec): (4441561/3486)
        HA last key lifetime sent(k): (4441561)
   ike_cookies: 00000000 00000000 00000000 00000000
   replay detection support: Y
   Status: STANDBY

inbound pcp sas:

outbound esp sas:
 spi: 0xD42904F0(3559458032)
   transform: esp-3des ,
   in use settings ={Tunnel, }
   conn id: 2011, flow_id: 11, crypto map: to-peer-outside
   sa timing: remaining key lifetime (k/sec): (4441561/3485)
        HA last key lifetime sent(k): (4441561)
   ike_cookies: 00000000 00000000 00000000 00000000
   IV size: 8 bytes
   replay detection support: Y
   Status: STANDBY

outbound ah sas:
 spi: 0x75251086(1965363334)
   transform: ah-md5-hmac ,
   in use settings ={Tunnel, }
   conn id: 2011, flow_id: 11, crypto map: to-peer-outside
   sa timing: remaining key lifetime (k/sec): (4441561/3485)
        HA last key lifetime sent(k): (4441561)
   ike_cookies: 00000000 00000000 00000000 00000000
   replay detection support: Y
   Status: STANDBY

outbound pcp sas:
```

Related Commands

Command	Description
crypto ipsec security-association	Configures the IPSec security associations.

show crypto ipsec security-association idle-time

To display the security association (SA) idle-time value configured for crypto map entry, use the **show crypto ipsec security-association idle-time** command in privileged EXEC mode.

show crypto ipsec security-association idle-time

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced in a release earlier than Cisco IOS Release 12.2(33)SRB.
12.2SX	This command was integrated into Cisco IOS Release 12.2SX.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Usage Guidelines

Use the **show crypto ipsec security-association idle-time** command to display the idle time.

When a router running the Cisco IOS software creates an IPsec SA for a peer, resources must be allocated to maintain the SA. The SA requires both memory and several managed timers. For idle peers, these resources are wasted. If enough resources are wasted by idle peers, the router could be prevented from creating new SAs with other peers. The IPsec Security Association Idle Timers feature introduces a configurable idle timer to monitor SAs for activity, allowing SAs for idle peers to be deleted. This increases the availability of the resources and improve scalability of Cisco IOS IPsec deployments.

Examples

The following is a sample output from the **show crypto ipsec security-association idle-time** command. The output is self-explanatory.

```
Router# show crypto ipsec security-association idle-time

Security association idletime: 567 seconds
```

Related Commands

Command	Description
show crypto ipsec security-association lifetime	Displays the SA lifetime value configured for a particular crypto map entry.

show crypto ipsec security-association lifetime

To display the security association (SA) lifetime value configured for a particular crypto map entry, use the **show crypto ipsec security-association lifetime** command in privileged EXEC mode.

show crypto ipsec security-association lifetime

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3 T	This command was introduced.\
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output for the **show crypto ipsec security-association lifetime** command:

```
Router# show crypto ipsec security-association lifetime

Security-association lifetime: 4608000 kilobytes/120 seconds
```

The following configuration was in effect when the previous **show crypto ipsec security-association lifetime** command was issued:

```
crypto ipsec security-association lifetime seconds 120
```

show crypto ipsec transform-set

To display the configured transform sets or active default transform sets, use the **show crypto ipsec transform-set** command in privileged EXEC mode.

show crypto ipsec transform-set [**tag** *transform-set-name*]

Syntax Description

tag *transform-set-name*	(Optional) Only the specified transform sets are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(13)T	The command output was expanded to include a warning message for users who try to configure an IP Security (IPsec) transform that the hardware does not support.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	The command output was expanded to include information about active default transform sets.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

There are two default transform sets supported in Cisco IOS k9 images only:

- Esp-aes esp-sha-hmac
- Esp-3des esp-sha-hmac

The **show crypto ipsec transform-set** command will display the default transform sets if there are no other transform set configured, you have not disabled the default transform sets by issuing the **no crypto ipsec default transform-set** command, and the crypto engine supports the encryption algorithm.

Examples

The following is sample output for the **show crypto ipsec transform-set** command when the default transform sets have been disabled with the **no crypto ipsec default transform-set** command:

```
Router# show crypto ipsec transform-set

Transform set combined-des-sha: {esp-des esp-sha-hmac}
   will negotiate = { Tunnel,  },

Transform set combined-des-md5: {esp-des esp-md5-hmac}
   will negotiate = { Tunnel,  },

Transform set t1: {esp-des esp-md5-hmac}
```

```
   will negotiate = {Tunnel,},

Transform set t100: {ah-sha-hmac}
   will negotiate = {Transport,},

Transform set t2: {ah-sha-hmac}
   will negotiate = {Tunnel,},
   { esp-des  }
   will negotiate = {Tunnel,},
```

The following configuration was in effect when the previous **show crypto ipsec transform-set** command was issued:

```
crypto ipsec transform-set combined-des-sha esp-des esp-sha-hmac
crypto ipsec transform-set combined-des-md5 esp-des esp-md5-hmac
crypto ipsec transform-set t1 esp-des esp-md5-hmac
crypto ipsec transform-set t100 ah-sha-hmac
 mode transport
crypto ipsec transform-set t2 ah-sha-hmac esp-des
no crypto ipsec default transform-set
```

The following sample output from the s**how crypto ipsec transform-set** command displays a warning message after a user tries to configure an IPsec transform that the hardware does not support:

```
Router# show crypto ipsec transform-set

Transform set transform-1:{ esp-256-aes esp-md5-hmac  }
   will negotiate = { Tunnel,  },

WARNING: encryption hardware does not support transform esp-aes 256 within IPSec transform
transform-1
```

The following is sample output for the **show crypto ipsec transform-set** command when the default transform sets are active and the crypto engine supports the encryption algorithm:

```
Router# show crypto ipsec transform-set

Transform set asset: { esp-256-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set aesset: { esp-256-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
```

Related Commands

Command	Description
show crypto ipsec default transform-set	Displays the default IPsec transform sets.
show crypto ipsec transform-set	Displays the configured transform sets.
show crypto map (IPsec)	Displays the crypto map configuration.

show crypto isakmp default policy

To display the default Internet Key Exchange (IKE) policies currently in use, use the **show crypto isakmp default policy** command in privileged EXEC mode.

show crypto isakmp default policy

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

If you have neither manually configured IKE policies with the **crypto isakmp policy** command nor issued the **no crypto isakmp default policy** command, IPsec will use the default IKE policies to negotiate IKE proposals. There are eight default IKE default policies supported (see Table 101). The default IKE policies define the following policy set parameters:

- The priority, 65507–65514, where 65507 is the highest priority and 65514 is the lowest priority.
- The authentication method, Rivest, Shamir, and Adelman (RSA) or preshared keys (PSK).
- The encryption method, Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES).
- The hash function, Secure Hash Algorithm (SHA-1) or Message-Digest algorithm 5 (MD5).
- The Diffie-Hellman (DH) group specification DH2 or DH5.
  - DH2 specifies the 768-bit Diffie-Hellman group.
  - DH5 specifies the 1536-bit Diffie-Hellman group.

Table 101 Default IKE Policies

Priority	Authentication	Encryption	Hash	Diffie-Hellman
65507	RSA	AES	SHA	DH5
65508	PSK	AES	SHA	DH5
65509	RSA	AES	MD5	DH5
65510	PSK	AES	MD5	DH5
65511	RSA	3DES	SHA	DH2
65512	PSK	3DES	SHA	DH2
65513	RSA	3DES	MD5	DH2
65514	PSK	3DES	MD5	DH2

If you have manually configured IKE policies and you issue the **show crypto isakmp default policy** command there is no output, since the default IKE policies are not in use.

Examples

The following example displays the eight default policies with protection suites of priorities 65507–65014. The default policies are displayed since there are no user configured policies, the default policies have not been disabled, and EzVPN is not configured.

```
Router# show crypto isakmp default policy

Default protection suite of priority 65507
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65508
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65509
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65510
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  pre-shared key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65511
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65512
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65513
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65514
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
```

The following example shows that there is no output from the **show crypto isakmp default policy** command when the default policies have been disabled.

```
Router(config)# no crypto isakmp default policy
! The default IKE policies have been disabled.
Router(config)# exit
Router# configure terminal
Router# show crypto isakmp default policy
Router#
! There is no output from the show crypto isakmp default policy command.
```

Related Commands

Command	Description
crypto isakmp policy	Defines an IKE policy.
no crypto isakmp default policy	Disables IKE default policies.
show crypto isakmp policy	Displays the parameters for each IKE policy.

show crypto isakmp key

To list the keyrings and their preshared keys, use the **show crypto isakmp key** command in privileged EXEC mode.

show crypto isakmp key

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(4)T	IPv6 address information was added to command output.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Examples

The following is sample output for the **show crypto isakmp key** command:

```
Router# show crypto isakmp key

Hostname/Address       Preshared Key
vpn1                   : 172.61.1.1          vpn1
vpn2                   : 10.1.1.1            vpn2
```

The following configuration was in effect when the above **show crypto isakmp key** command was issued:

```
crypto keyring vpn1
  pre-shared-key address 172.16.1.1 key vpn1
crypto keyring vpn2
  pre-shared-key address 10.1.1.1 key vpn2
```

Table 102 describes significant fields in the **show crypto isakmp key** profile.

Table 102 show crypto isakmp key Field Descriptions

Field	Description
Hostname/Address	The preshared key host name or address.
Preshared Key	The preshared key.
keyring	Name of the crypto keyring. The global keys are listed in the default keyring.
VRF string	The Virtual Private Network routing and forwarding (VRF) of the keyring. If the keyring does not have a VRF, an empty string is printed.

show crypto isakmp peers

To display the Internet Security Association and Key Management Protocol (ISAKMP) peer descriptions, use the **show crypto isakmp peers** command in privileged EXEC mode.

show crypto isakmp peers [*ipaddress* | *ipv6address* | **config** [*peername*]]

Syntax Description

ipaddress	(Optional) The IP address of the specific peer. **Note** If the optional *ipaddress* argument is not included with the command, a summarization of all peers is displayed.
ipv6address	(Optional) The IPv6 address of the specific peer.
config	(Optional) Displays detailed information about all peers or a specific peer.
peername	(Optional) The peer name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(4)T	The **config** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.4(11)T	The **show crypto isakmp peer** command name was changed to **show crypto isakmp peers**.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 on the Cisco ASR 1000 Series Routers.

Usage Guidelines

Before you can use the **config** keyword, the following commands must be enabled for the accounting update to work correctly: **aaa accounting update** with **new info** keyword and **radius-server vsa send** with **accounting** keyword.

Examples

The following output example shows information about the peer named "This-is-another-peer-at-10-1-1-3":

```
Router# show crypto isakmp peers

Peer: 10.1.1.3 Port: 500
 Description: This-is-another-peer-at-10-1-1-3
 Phase1 id: 10.1.1.3
```

In the following example, the **config** keyword is used to display all manageability information for an Easy VPN remote device. Cisco Easy VPN is an IP Security (IPsec) virtual private network (VPN) solution supported by Cisco routers and security appliances. It greatly simplifies VPN deployment for remote offices and mobile workers. The fields are self-explanatory.

```
Router# show crypto isakmp peers config

Client-Public-Addr=192.168.10.2:500; Client-Assigned-Addr=172.16.1.209;
Client-Group=branch; Client-User=branch; Client-Hostname=branch.; Client-Platform=Cisco
1711; Client-Serial=FOC080210E2 (412454448); Client-Config-Version=11;
Client-Flash=33292284; Client-Available-Flash=10202680; Client-Memory=95969280;
Client-Free-Memory=14992140; Client-Image=flash:c1700-advipservicesk9-mz.ef90241;

Client-Public-Addr=192.168.10.3:500; Client-Assigned-Addr=172.16.1.121;
Client-Group=store; Client-User=store; Client-Hostname=831-storerouter.;
Client-Platform=Cisco C831; Client-Serial=FOC08472UXR (1908379618);
Client-Config-Version=2; Client-Flash=24903676; Client-Available-Flash=5875028;
Client-Memory=45298688; Client-Free-Memory=6295596;
Client-Image=flash:c831-k9o3y6-mz.ef90241
```

Related Commands

Command	Description
aaa accounting update	Enables the periodic interim accounting records to be sent to the accounting server.
radius-server vsa send	Configures the network access server (NAS) to recognize and use vendor-specific attributes (VSAs).
clear crypto session	Deletes crypto sessions (IPSec and IKE) SAs.
show crypto session	Displays status information for active crypto sessions in a router.

show crypto isakmp policy

To display the parameters for each Internet Key Exchange (IKE) policy, use the **show crypto isakmp policy** command in privileged EXEC mode.

show crypto isakmp policy

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3T	This command was introduced.
12.2(13)T	The command output was expanded to include a warning message for users who try to configure an IKE encryption method that the hardware does not support.
12.4(4)T	Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	The command output was expanded to include default IKE policies.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

There are eight default IKE default policies supported with protection suites of priorities 65507–65514, where 65507 is the highest priority and 65514 is the lowest priority. If you have neither manually configured IKE policies with the **crypto isakmp policy** command nor disabled the default IKE policies by issuing the **no crypto isakmp default policy** command, the default IKE policies will be displayed when the **show crypto isakmp policy** command is issued.

Examples

The following is sample output from the **show crypto isakmp policy** command, after two IKE policies have been configured (with priorities 15 and 20, respectively):

```
Router# show crypto isakmp policy

Protection suite priority 15
        encryption algorithm:    DES - Data Encryption Standard (56 bit keys)
        hash algorithm:  Message Digest 5
        authentication method:   Rivest-Shamir-Adleman Signature
        Diffie-Hellman Group:    #2 (1024 bit)
        lifetime:      5000 seconds, no volume limit
Protection suite priority 20
        encryption algorithm:    DES - Data Encryption Standard (56 bit keys)
        hash algorithm: Secure Hash Standard
        authentication method:   preshared Key
```

```
        Diffie-Hellman Group:    #1 (768 bit)
        lifetime:      10000 seconds, no volume limit
Default protection suite
        encryption algorithm:    DES - Data Encryption Standard (56 bit keys)
        hash algorithm: Secure Hash Standard
        authentication method:   Rivest-Shamir-Adleman Signature
        Diffie-Hellman Group:    #1 (768 bit)
        lifetime:      86400 seconds, no volume limit
```

Note Although the output shows "no volume limit" for the lifetimes, you can currently configure only a time lifetime (such as 86,400 seconds); volume limit lifetimes are not used.

The following sample output from the **show crypto isakmp policy** command displays a warning message after a user tries to configure an IKE encryption method that the hardware does not support:

```
Router# show crypto isakmp policy

Protection suite of priority 1
        encryption algorithm:  AES - Advanced Encryption Standard (256 bit keys).
WARNING:encryption hardware does not support the configured
encryption method for ISAKMP policy 1
        hash algorithm:        Secure Hash Standard
        authentication method: Pre-Shared Key
        Diffie-Hellman group:  #1 (768 bit)
        lifetime:              3600 seconds, no volume limit
```

The following sample output from the **show crypto isakmp policy** command displays the default IKE policies. The manually configured IKE policies with priorities 10 and 20 have been removed.

```
Router(config)# no crypto isakmp policy 10
Router(config)# no crypto isakmp policy 20
Router(config)# exit
R1# show crypto isakmp policy

Default IKE policy
Protection suite of priority 65507
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65508
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65509
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65510
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65511
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
```

```
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65512
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65513
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65514
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
```

The field descriptions in the display are self-explanatory.

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
group (IKE policy)	Specifies the DH group identifier within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
show crypto isakmp default policy	Displays the default IKE policies.

show crypto isakmp profile

To list all the Internet Security Association and Key Management Protocol (ISAKMP) profiles that are defined on a router, use the **show crypto isakmp profile** command in privileged EXEC mode.

show crypto isakmp profile [**tag** *profilename* | **vrf** *vrfname*]

Syntax Description

tag *profilename*	(Optional) Displays ISAKMP profile details specified by the profile name.
vrf *vrfname*	(Optional) Displays ISAKMP profile details specified by the VPN routing/forwarding instance (VRF) name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(4)T	IPv6 support was added.
12.4(11)T	The **tag** *profilename* and **vrf** *vrfname* keywords and arguments were added.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Examples

The following is sample output from the **show crypto isakmp profile** command:

```
Router# show crypto isakmp profile

ISAKMP PROFILE vpn1-ra
   Identities matched are:
group vpn1-ra
   Identity presented is: ip-address
```

The following sample output shows information for an IPv6 router:

```
Router# show crypto isakmp profile

ISAKMP PROFILE tom
Identities matched are:
ipv6-address 2001:0DB8:0:1::1/32
Certificate maps matched are:
Identity presented is: ipv6-address fqdn
keyring(s): <none>
trustpoint(s): <all>
```

Table 103 describes the significant fields shown in the display.

Table 103 show crypto isakmp profile Field Descriptions

Field	Description
ISAKMP PROFILE	Name of the ISAKMP profile.

Table 103 show crypto isakmp profile Field Descriptions

Field	Description
Identities matched are:	Lists all identities that the ISAKMP profile will match.
Identity presented is:	The identity that the ISAKMP profile will present to the remote endpoint.

The following configuration was in effect when the preceding **show crypto isakmp profile** command was issued:

```
crypto isakmp profile vpn1-ra
 vrf vpn1
 self-identity address
 match identity group vpn1-ra
 client authentication list aaa-list
 isakmp authorization list aaa
 client configuration address initiate
 client configuration address respond
```

Related Commands

Command	Description
show crypto isakmp key	Lists the keyrings and their preshared keys.

show crypto isakmp sa

To display current Internet Key Exchange (IKE) security associations (SAs), use the **show crypto isakmp sa** command in privileged EXEC mode.

show crypto isakmp sa [**active** | **standby** | **detail** | **nat**] [**vrf** *vrfname*]

Syntax Description

active	(Optional) Displays high availability- (HA-) enabled Internet Security Association and Key Management Protocol (ISAKMP) SAs that are in the active state.
standby	(Optional) Displays HA-enabled ISAKMP SAs that are in the standby state.
detail	(Optional) Displays all existing IKE SAs, whether in an active or standby state.
nat	(Optional) Displays IKE SAs that have undergone network address translation (NAT).
vrf *vrfname*	(Optional) Displays IKE SA details about the specified VRF. • The *vrfname* value is the name of the VRF.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3 T	This command was introduced.
12.3(11)T	The **active** and **standby** keywords were added.
12.4(4)T	IPv6 information was added to the command output. The **detail** and **nat** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.4(11)T	The **vrf** *vrfname* keyword and argument were added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If neither the **active** keyword nor the **standby** keyword is specified, current SAs for all configured routers will be shown. Use the **nat** keyword to display the IP address and port address of a remote peer when NAT is used.

Examples

The following sample output shows the SAs of both the active and standby devices:

```
Router# show crypto isakmp sa

dst             src             state          conn-id slot status
10.165.201.3   10.165.200.225 QM_IDLE              2    0 STDBY
10.0.0.1        10.0.0.2        QM_IDLE             1    0 ACTIVE
```

The following sample output shows the SAs of only the active device:

```
Router# show crypto isakmp sa active

dst             src             state          conn-id slot status
10.165.201.3    10.165.200.225 QM_IDLE             5    0 ACTIVE
```

The following sample output shows the SAs of only the standby device:

```
Router# show crypto isakmp sa standby

dst             src             state          conn-id slot status
10.165.201.3    10.165.200.225 QM_IDLE             5    0 STDBY
10.165.201.3    10.165.200.225 QM_IDLE             1    0 STDBY
```

The following sample output shows the SAs of an active IPv6 device. The IPv4 device is inactive.

```
Router# show crypto isakmp sa detail

Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local           Remote          I-VRF    Status Encr Hash Auth DH
Lifetime Cap.

IPv6 Crypto ISAKMP SA

  dst: 3FFE:2002::A8BB:CCFF:FE01:2C02
  src: 3FFE:2002::A8BB:CCFF:FE01:9002
  conn-id: 1001  I-VRF:          Status: ACTIVE Encr: des  Hash: sha  Auth:
psk
  DH: 1  Lifetime: 23:45:00 Cap: D    Engine-id:Conn-id = SW:1

  dst: 3FFE:2002::A8BB:CCFF:FE01:2C02
  src: 3FFE:2002::A8BB:CCFF:FE01:9002
  conn-id: 1002  I-VRF:          Status: ACTIVE Encr: des  Hash: sha  Auth:
psk
  DH: 1  Lifetime: 23:45:01 Cap: D    Engine-id:Conn-id = SW:2
```

Table 104 through Table 107 show the various states that may be displayed in the output of the **show crypto isakmp sa** command. When an Internet Security Association and Key Management Protocol (ISAKMP) SA exists, it will most likely be in its quiescent state (QM_IDLE). For long exchanges, some of the main mode (MM_xxx) states may be observed.

Table 104 States in Main Mode Exchange

State	Explanation
MM_NO_STATE	The ISAKMP SA has been created, but nothing else has happened yet. It is “larval” at this stage—there is no state.
MM_SA_SETUP	The peers have agreed on parameters for the ISAKMP SA.

Table 104 States in Main Mode Exchange

State	Explanation
MM_NO_STATE	The ISAKMP SA has been created, but nothing else has happened yet. It is "larval" at this stage—there is no state.
MM_KEY_EXCH	The peers have exchanged Diffie-Hellman public keys and have generated a shared secret. The ISAKMP SA remains unauthenticated.
MM_KEY_AUTH	The ISAKMP SA has been authenticated. If the router initiated this exchange, this state transitions immediately to QM_IDLE, and a Quick Mode exchange begins.

Table 105 States in Aggressive Mode Exchange

State	Explanation
AG_NO_STATE	The ISAKMP SA has been created, but nothing else has happened yet. It is "larval" at this stage—there is no state.
AG_INIT_EXCH	The peers have done the first exchange in aggressive mode, but the SA is not authenticated.
AG_AUTH	The ISAKMP SA has been authenticated. If the router initiated this exchange, this state transitions immediately to QM_IDLE, and a quick mode exchange begins.

Table 106 States in Quick Mode Exchange

State	Explanation
QM_IDLE	The ISAKMP SA is idle. It remains authenticated with its peer and may be used for subsequent quick mode exchanges. It is in a quiescent state.

Table 107 show crypto isakmp sa Field Descriptions

Field	Description
f_vrf/i_vrf (not shown)	The front door virtual routing and forwarding (FVRF) and the inside VRF (IVRF) of the IKE SA. If the FVRF is global, the output shows f_vrf as an empty field.

Related Commands

Command	Description
crypto isakmp policy	Defines an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.

show crypto key mypubkey rsa

To display the RSA public keys of your router, use the **show crypto key mypubkey rsa** command in privileged EXEC mode.

show crypto key mypubkey rsa

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3 T	This command was introduced.
12.3(7)T	The show output was modified to display whether an RSA key is protected (encrypted) and locked or unlocked.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
15.0(1)M	This command was modified to display whether redundancy is specified in the **crypto_key_generate_rsa command**.

Usage Guidelines

This command displays the RSA public keys of your router.

Note Secure Shell (SSH) may generate an additional RSA keypair if you generate a keypair on a router having no RSA keys. The additional keypair is used only by SSH and will have a name such as {*router_FQDN*}.server. For example, if a router name is "router1.cisco.com," the keyname is "router1.cisco.com.server."

Examples

The following is sample output from the **show crypto key mypubkey rsa** command. Special usage RSA keys were previously generated for this router using the **crypto key generate rsa** command.

```
% Key pair was generated at: 06:07:49 UTC Jan 13 1996
Key name: myrouter.example.com
 Usage: Signature Key
 Key Data:
  005C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B 55D6AB22
  04AEF1BA A54028A6 9ACC01C5 129D99E4 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
  BD62A8A9 FA603DD2 E2A8A6F8 98F76E28 D58AD221 B583D7A4 71020301 0001

% Key pair was generated at: 06:07:50 UTC Jan 13 1996
Key name: myrouter.example.com
 Usage: Encryption Key
 Key Data:
  00302017 4A7D385B 1234EF29 335FC973 2DD50A37 C4F4B0FD 9DADE748 429618D5
  18242BA3 2EDFBDD3 4296142A DDF7D3D8 08407685 2F2190A0 0B43F1BD 9A8A26DB
  07953829 791FCDE9 A98420F0 6A82045B 90288A26 DBC64468 7789F76E EE21
```

The following example shows how to encrypt the RSA key "pki1-72a.cisco.com." Thereafter, the **show crypto key mypubkey rsa** command is issued to verify that the RSA key is encrypted (protected) and unlocked.

```
Router(config)# crypto key encrypt rsa name pki1-72a.cisco.com passphrase cisco1234
Router(config)# exit
Router# show crypto key mypubkey rsa

% Key pair was generated at:00:15:32 GMT Jun 25 2003
Key name:pki1-72a.cisco.com
Usage:General Purpose Key
*** The key is protected and UNLOCKED. ***
Key is not exportable.
Key Data:
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E0CC9A 1D23B52C
CD00910C ABD392AE BA6D0E3F FC47A0EF 8AFEE340 0EC1E62B D40E7DCC
23C4D09E
03018B98 E0C07B42 3CFD1A32 2A3A13C0 1FF919C5 8DE9565F 1F020301 0001
% Key pair was generated at:00:15:33 GMT Jun 25 2003
Key name:pki1-72a.cisco.com.server
Usage:Encryption Key
Key is exportable.
Key Data:
307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00D3491E 2A21D383
854D7DA8 58AFBDAC 4E11A7DD E6C40AC6 66473A9F 0C845120 7C0C6EC8 1FFF5757
3A41CE04 FDCB40A4 B9C68B4F BC7D624B 470339A3 DE739D3E F7DDB549 91CD4DA4
DF190D26 7033958C 8A61787B D40D28B8 29BCD0ED 4E6275C0 6D020301 0001
Router#
```

The following example shows how to lock the key "pki1-72a.cisco.com." Thereafter, the **show crypto key mypubkey rsa** command is issued to verify that the key is protected (encrypted) and locked.

```
Router# crypto key lock rsa name pki1-72a.cisco.com passphrase cisco1234
!
Router# show crypto key mypubkey rsa

% Key pair was generated at:20:29:41 GMT Jun 20 2003
Key name:pki1-72a.cisco.com
Usage:General Purpose Key
*** The key is protected and LOCKED. ***
Key is exportable.
Key Data:
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00D7808D C5FF14AC
0D2B55AC 5D199F2F 7CB4B355 C555E07B 6D0DECBE 4519B1F0 75B12D6F 902D6E9F
B6FDAD8D 654EF851 5701D5D7 EDA047ED 9A2A619D 5639DF18 EB020301 0001
```

The string "Redundancy enabled" in the following example indicates that the **redundancy** keyword was specified when the key was generated by the **crypto_key_generate_rsa command**.

```
Router#show crypto key mypubkey rsa MYKEYS
% Key pair was generated at: 07:38:04 GMT Oct 02 2009
Key name: MYKEYS
 Storage Device: not specified
 Usage: General Purpose Key
 Key is not exportable. Redundancy enabled.
 Key Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00A63726 28C9EE7D
  A89AF6E1 5B42A854 A76EDF9F 35681024 A7868113 B93E2384 EF15CD78 8467A797
  F946268F 067FF15E A1734BE6 3E3444C2 BAE00618 BCAED5A3 BB020301 0001
```

Related Commands

Command	Description
crypto key encrypt rsa	Encrypts the RSA private key.
crypto key generate rsa	Generates RSA key pairs.
crypto key lock rsa	Locks the RSA private key in a router.

show crypto key pubkey-chain rsa

To display the RSA public keys of the peer that are stored on the router, use the **show crypto key pubkey-chain rsa** command in user EXEC mode or privileged EXEC mode.

show crypto key pubkey-chain rsa [**address** *key-address* | **name** *key-name* | **vrf** *vrf-name* [**address** *ip-address*]]

Syntax Description

address *key-address*	(Optional) Address of a specific key to view.
name *key-name*	(Optional) Name of a specific key to view.
vrf *vrf-name*	(Optional) Name of a specific Virtual Private Network (VPN) Routing and Forwarding (VRF) instance for which to display keys.
address *ip-address*	(Optional) IP address belonging to a VRF instance.

Command Default

Information is displayed for all RSA public keys stored on the router.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.3T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The keys that are displayed include peers' RSA public keys that are manually configured at the router and keys that are received by the router via other means (such as by a certificate, if certification authority support is configured).

If a router reboots, any keys derived by certificates are lost. This is because the router requests certificates again (then the keys are derived again).

Examples

The following example shows how to display information for all RSA public keys stored on the router:

```
Router# show crypto key pubkey-chain rsa

Codes: M - Manually Configured, C - Extracted from certificate

Code Usage         IP-address            Keyring          Name
M    Signature     209.165.200.225       default          myrouter.example.com
M    Encryption    209.165.202.129       default          myrouter.example.com
```

```
C     Signature    209.165.200.225        default          routerA.example.com
C     Encryption   209.165.202.129        default          routerA.example.com
C     General      209.165.200.225        default          routerB.domain1.com
```

The example above shows manually configured special usage RSA public keys for the peer myrouter.example.com. This sample also indicates certificate support and therefore shows three keys obtained from peers' certificates: special usage keys for peer routerA.example.com and a general purpose key for peer routerB.domain1.com.

The following example shows how to display keys for a specific VRF instance.

```
Router# show crypto key pubkey-chain rsa vrf
Code Usage         IP-Address/VRF         Keyring          Name
M    General       209.165.200.225        default          Key_1
M    General       209.165.202.129        default          Key_2
```

The following example shows how to display details for a key named somerouter.example.com:

```
Router# show crypto key pubkey-chain rsa name somerouter.example.com

Key name: somerouter.example.com
Key address: 209.165.200.225
 Usage: Signature Key
 Source: Manual
 Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B 55D6AB22
  04AEF1BA A54028A6 9ACC01C5 129D99E4 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
  BD62A8A9 FA603DD2 E2A8A6F8 98F76E28 D58AD221 B583D7A4 71020301 0001

Key name: somerouter.example.com
Key address: 209.165.200.225
 Usage: Encryption Key
 Source: Manual
 Data:
  00302017 4A7D385B 1234EF29 335FC973 2DD50A37 C4F4B0FD 9DADE748 429618D5
  18242BA3 2EDFBDD3 4296142A DDF7D3D8 08407685 2F2190A0 0B43F1BD 9A8A26DB
  07953829 791FCDE9 A98420F0 6A82045B 90288A26 DBC64468 7789F76E EE21
```

Note The Source field in the above example displays "Manual," which means that the keys were manually configured on the router (and not received in the peer's certificate).

The following example shows how to display details for a key with address 209.165.202.129:

```
Router# show crypto key pubkey-chain rsa address 209.165.202.129

Key name: routerB.example.com
Key address: 209.165.202.129
 Usage: General Purpose Key
 Source: Certificate
 Data:
  0738BC7A 2BC3E9F0 679B00FE 53987BCC 01030201 42DD06AF E228D24C 458AD228
  58BB5DDD F4836401 2A2D7163 219F882E 64CE69D4 B583748A 241BED0F 6E7F2F16
  0DE0986E DF02031F 4B0B0912 F68200C4 C625C389 0BFF3321 A2598935 C1B1
```

Note The Source field in the above example displays "Certificate," which means that the keys were received by the router from the certificate authority.

Table 108 describes the significant fields shown in the displays.

Table 108 show crypto key pubkey-chain rsa Field Descriptions

Field	Description
Code	Source of the key: M (manually configured at the router) or C (received by the router via a certificate).
Usage	Purpose of the key: general purpose, signature, or encryption).
IP-Address/VRF	IP address or VRF of the key.
Keyring	Name of the keyring that stores the key. The possible values are either the name of a user-defined keyring or default (the default keyring).
Name	Name of the key. For manually inserted keys (code M), this name is manually configured. For keys that are extracted from the certificate (code C) the name is the subject name in the certificate itself.
Data	The contents of the key itself.

Related Commands

Command	Description
crypto key pubkey-chain rsa	Enters public key configuration mode (so you can manually specify other devices' RSA public keys).
rsa-pubkey	Defines the RSA manual key to be used for encryption or signature during IKE authentication.

show crypto map (IPsec)

To display the crypto map configuration, use the **show crypto map** command in user EXEC or privileged EXEC mode.

show crypto map [**gdoi fail-close** *map-name* | **interface** *interface* | **tag** *map-name*]

Syntax Description

gdoi	(Optional) Displays information about the status of the Group Domain of Interpretation (GDOI) fail-close mode.
fail-close	Specifies the list of crypto maps configured with the fail-close mode.
map-name	Name of the specified crypto map.
interface *interface*	(Optional) Displays only the crypto map set that is applied to the specified interface.
tag	(Optional) Displays only the crypto map set that is specified.

Command Default

No crypto maps are displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.2	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T. The output was modified to display the crypto input and output Access Control Lists (ACLs) that have been configured.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T. IPv6 address information was added to command output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command was integrated into Cisco IOS Release 12.2SX. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T. The default transform set information was added to command output.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T. The **gdoi fail-close** keywords and the *map-tag* arguments were added.
Cisco IOS XE Release 2.3	This command was modified. It was integrated into Cisco IOS XE Release 2.3.

Usage Guidelines

The **show crypto map** command allows you to specify a particular crypto map. The crypto maps shown in the command output are dynamically generated; you need not configure crypto maps in order for them to appear in this command output.

Two default transform sets are supported in Cisco IOS K9 images only:

- Esp-aes esp-sha-hmac
- Esp-3des esp-sha-hmac

The **show crypto map** command displays the default transform sets if no other transform sets are configured for the crypto map, if you have not disabled the default transform sets by issuing the **no crypto ipsec default transform-set** command, and if the crypto engine supports the encryption algorithm.

Examples

The following example shows that crypto input and output ACLs have been configured:

```
Router# show crypto map

Crypto Map "test" 10 ipsec-isakmp
 Peer
 Extended IP access list ipsec_acl
  access-list ipsec_acl permit ip 192.168.2.0 0.0.0.255 192.168.102.0 0.0.0.255
 Extended IP access check IN list 110
  access-list 110 permit ip host 192.168.102.47 192.168.2.0 10.0.0.15
  access-list 110 permit ip host 192.168.102.47 192.168.2.32 10.0.0.15
  access-list 110 permit ip host 192.168.102.47 192.168.2.64 10.0.0.15
  access-list 110 permit ip host 192.168.102.57 192.168.2.0 10.0.0.15
  access-list 110 permit ip host 192.168.102.57 192.168.2.32 10.0.0.15
  access-list 110 permit ip host 192.168.102.57 192.168.2.64 10.0.0.15
 Extended IP access check OUT list 120
  access-list 120 permit ip 192.168.2.0 10.0.0.15 host 192.168.102.47
  access-list 120 permit ip 192.168.2.32 10.0.0.15 host 192.168.102.47
  access-list 120 permit ip 192.168.2.64 10.0.0.15 host 192.168.102.47
  access-list 120 permit ip 192.168.2.0 10.0.0.15 host 192.168.102.57
  access-list 120 permit ip 192.168.2.32 10.0.0.15 host 192.168.102.57
  access-list 120 permit ip 192.168.2.64 10.0.0.15 host 192.168.102.57
 Current peer: 10.0.0.2
 Security association lifetime: 4608000 kilobytes/3600 seconds
 PFS (Y/N): N
 Transform sets=test
 Interfaces using crypto map test:
  Serial0/1
```

Table 109 describes the significant fields shown in the display.

Table 109 show crypto map Field Descriptions

Field	Description
Peer	Possible peers that are configured for this crypto map entry.
Extended IP access list	Access list that is used to define the data packets that need to be encrypted. Packets that are denied by this access list are forwarded but not encrypted. The “reverse” of this access list is used to check the inbound return packets, which are also encrypted. Packets that are denied by the “reverse” access list are dropped because they should have been encrypted but were not.

Table 109 show crypto map Field Descriptions (continued)

Field	Description
Extended IP access check	Access lists that are used to more finely control which data packets are allowed into or out of the IPsec tunnel. Packets that are allowed by the "Extended IP access list" ACL but denied by the "Extended IP access list check" ACL are dropped.
Current peer	Current peer that is being used for this crypto map entry.
Security association lifetime	Number of bytes that are allowed to be encrypted or decrypted or the age of the security association before new encryption keys must be negotiated.
PFS	(Perfect Forward Secrecy) If the field is marked as 'Yes', the Internet Security Association and Key Management Protocol (ISAKMP) SKEYID-d key is renegotiated each time security association (SA) encryption keys are renegotiated (requires another Diffie-Hillman calculation). If the field is marked as 'No', the same ISAKMP SKEYID-d key is used when renegotiating SA encryption keys. ISAKMP keys are renegotiated on a separate schedule, with a default time of 24 hours.
Transform sets	List of transform sets (encryption, authentication, and compression algorithms) that can be used with this crypto map.
Interfaces using crypto map test	Interfaces to which this crypto map is applied. Packets that are leaving from this interface are subject to the rules of this crypto map for encryption. Encrypted packets may enter the router on any interface, and they are decrypted. Nonencrypted packets that are entering the router through this interface are subject to the "reverse" crypto access list check.

The following example displays output from the **show crypto map** command. No transform sets are configured for the crypto map "mymap," the default transform sets are enabled, and the crypto engine supports the encryption algorithm.

```
Router# show crypto map

Crypto Map "mymap" 1 ipsec-isakmp
        Peer = 209.165.201.1
        Extended IP access list 102
            access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                #$!default_transform_set_1:  { esp-aes esp-sha-hmac  } ,
                #$!default_transform_set_0:  { esp-3des esp-sha-hmac  } ,
        }
        Reverse Route Injection Enabled
        Interfaces using crypto map mymap:
```

The following example displays output of the **show crypto map** command. No transform sets configured for the crypto map "mymap" and the default transform sets have been disabled.

```
Router(config)# no crypto ipsec default transform-set
Router(config)# exit
Router# configure terminal
Router# show crypto map

Crypto Map "mymap" 1 ipsec-isakmp
        Peer = 209.165.201.1
        Extended IP access list 102
            access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
        }


! There are no transform sets for the crypto map "mymap."
        Reverse Route Injection Enabled
        Interfaces using crypto map mymap:
```

The following example displays output for the **show crypto map** command and **gdoi fail-close** keywords (**show crypto map gdoi fail-close**). Fail-close has been activated. In addition, an implicit "permit ip any any" entry is configured, causing any traffic other than Telnet and Open Shortest Path First (OSPF) to be dropped:

```
Router# show crypto map gdoi fail-close 23

Crypto Map: "svn"
        Activate: yes
        Fail-Close Access-List: (Deny = Forward In Clear, Permit = Drop)
            access-list 105 deny tcp any port = 23 any
            access-list 105 deny ospf any any
```

Related Commands

Command	Description
show crypto ipsec default transform-set	Displays the default IPsec transform sets.
show crypto ipsec transform-set	Displays the configured transform sets.

show crypto mib ipsec flowmib endpoint

To display the IP Security (IPsec) phase-2 tunnel endpoint table, use the **show crypto mib ipsec flowmib endpoint** command in privileged EXEC mode.

show crypto mib ipsec flowmib endpoint [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

The IPsec phase-2 tunnel endpoint table contains an entry for each active endpoint associated with an IPsec phase-2 tunnel.

Examples

The following example displays the IPsec phase 2 tunnel endpoint table for all VRFs:

```
Router# show crypto mib ipsec flowmib endpoint

vrf Global
  Index:               1
  Local type:          Single IP address
  Local address:       192.1.2.1
  Protocol:            0
  Local port:          0
  Remote type:         Single IP address
  Remote address:      192.1.2.2
  Remote port:         0

  Index:               2
  Local type:          Subnet
  Local address:       192.1.3.0 255.255.255.0
  Protocol:            0
  Local port:          0
  Remote type:         Subnet
  Remote address:      192.1.3.0 255.255.255.0
  Remote port:         0
```

Table 110 describes the significant fields shown in the display.

Table 110 show crypto mib ipsec flowmib endpoint Field Descriptions

Field	Description
Index	The number of the endpoint associated with the IPsec phase-2 tunnel table. The value of this index is a number which begins at one and is incremented with each endpoint associated with an IPsec phase-2 tunnel. The index value will wrap at 2,147,483,647.
Local type	The local endpoint identity type. The three possible values are a single IP address, an IP address range, or an IP subnet.
Local address	The first IP address of the local endpoint. If the local endpoint type is a single IP address, then the local address is the value of the IP address. If the local endpoint type is an IP address range, then the local address is the value of beginning IP address of the range. If the local endpoint type is an IP subnet, then the local address is the value of the subnet.
Protocol	The local endpoint traffic protocol number.
Local port	The local endpoint traffic port number.
Remote type	The remote endpoint identity type. The three possible values are a single IP address, an IP address range, or an IP subnet.
Remote address	The first IP address of the remote endpoint. If the remote endpoint type is a single IP address, then the remote address is the value of the IP address. If the remote endpoint type is an IP address range, then the remote address is the value of beginning IP address of the range. If the remote endpoint type is an IP subnet, then the remote address is the value of the subnet.
Remote port	The remote endpoint traffic port number.

Related Commands

Command	Description
show crypto mib ipsec flowmib failure	Displays statistics associated with IPsec phase-2 failure.
show crypto mib ipsec flowmib global	Displays IPsec phase-2 global statistics.
show crypto mib ipsec flowmib history	Displays statistics associated with previously active IPsec phase-2 tunnels.
show crypto mib ipsec flowmib spi	Displays the IPsec phase-2 security protection index (SPI) table.
show crypto mib ipsec flowmib tunnel	Displays statistics for all active IPsec phase-2 tunnels.

show crypto mib ipsec flowmib failure

To display statistics associated with IP Security (IPsec) phase-2 failure, use the **show crypto mib ipsec flowmib failure** command in privileged EXEC mode.

show crypto mib ipsec flowmib failure [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following example displays the IPsec phase 2 MIB failure table for all indexes and VRFs:

```
Router# show crypto mib ipsec flowmib failure

vrf Global
  Index:                        1
  Reason:                       Operation request
  Failure time since reset:     00:25:18
  Src address:                  192.1.2.1
  Destination address:          192.1.2.2
  SPI:                          0
```

Table 111 describes the significant fields shown in the display.

Table 111 show crypto mib ipsec flowmib failure Field Descriptions

Field	Description
Index	The IPsec phase-2 failure table index. The value of the index is a number that begins at one and is incremented with each IPsec phase-1 failure. The index value will wrap at 2,147,483,647.
Reason	The reason for the failure, which are: • 1—All other reasons. • 2—An internal error occurred. • 3—A peer encoding error occurred. • 4—A proposal failure occurred. • 5—A protocol use failure occurred. • 6—The SA did not exist. • 7—A decryption failure occurred. • 8—An encryption failure occurred. • 9—An inbound authentication failure occurred. • 10—An outbound authentication failure occurred. • 11—A compression failure occurred. • 12—A system capacity failure occurred. • 13—A peer delete request was received. • 14—The contact with the peer was lost. • 15—The sequence rolled over. • 16—The operator requested tunnel termination.
Failure time since reset	The value of sysUpTime in hundredths of seconds at the time of the failure

Related Commands

Command	Description
show crypto mib ipsec flowmib endpoint	Displays IPsec phase-2 tunnel endpoint table.
show crypto mib ipsec flowmib global	Displays IPsec phase-2 global statistics.
show crypto mib ipsec flowmib history	Displays statistics associated with previously active IPsec phase-2 tunnels.
show crypto mib ipsec flowmib spi	Displays the IPsec phase-2 SPI table.
show crypto mib ipsec flowmib tunnel	Displays statistics for all active IPsec phase-2 tunnels.

show crypto mib ipsec flowmib global

To display IP Security (IPsec) phase-2 global statistics, use the **show crypto mib ipsec flowmib global** command in privileged EXEC mode.

show crypto mib ipsec flowmib global [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following example displays IPsec phase 2 global statistics for all VRFs:

```
Router# show crypto mib ipsec flowmib global

 vrf Global
  Active Tunnels:                   2
  Previous Tunnels:                 0
  In octets:                        800
  Out octets:                       1408
  In packets:                       8
  Out packets:                      8
  Uncompressed encrypted bytes:     1408
  In packets drops:                 0
  Out packets drops:                2
  In replay drops:                  0
  In authentications:               8
  Out authentications:              8
  In decrypts:                      8
  Out encrypts:                     8
  Compressed bytes:                 0
  Uncompressed bytes:               0
  In uncompressed bytes:            0
  Out uncompressed bytes:           0
  In decrypt failures:              0
  Out encrypt failures:             0
  No SA failures:                   0
  Protocol use failures:            0
  System capacity failures:         0
  In authentication failures:          0
  Out authentication failures:         0
```

Table 112 describes the significant fields shown in the display.

Table 112 show crypto mib ipsec flowmib global Field Descriptions

Field	Description
Active Tunnels	The total number of currently active IPsec phase-2 tunnels.
Previous Tunnels	The total number of previously active IPsec phase-2 tunnels.
In octets	The total number of octets received by all current and previous IPsec phase-2 tunnels. The total number is accumulated before determining whether or not the packet should be decompressed.
Out octets	The total number of octets sent by all current and previous IPsec phase-2 Tunnels. The total number is accumulated after determining whether or not the packet should be compressed.
In packets drops	The total number of packets dropped during receive processing by all current and previous IPsec phase-2 tunnels. The total number does not include packets dropped due to anti-replay processing.
Out packets drops	The total number of packets dropped during send processing by all current and previous IPsec phase-2 tunnels.
In replay drops	The total number of packets dropped during receive processing due to anti-replay processing by all current and previous IPsec phase-2 tunnels.
No SA failures	The total number of non-existent SA inbound failures that occurred during processing of all current and previous IPsec phase-2 tunnels.

Related Commands

Command	Description
show crypto mib ipsec flowmib endpoint	Displays IPsec phase-2 tunnel endpoint table.
show crypto mib ipsec flowmib failure	Displays statistics associated with IPsec phase-2 failure.
show crypto mib ipsec flowmib history	Displays statistics associated with previously active IPsec phase-2 tunnels.
show crypto mib ipsec flowmib spi	Displays the IPsec phase-2 SPI table.
show crypto mib ipsec flowmib tunnel	Displays statistics for all active IPsec phase-2 tunnels.

show crypto mib ipsec flowmib history

To display statistics associated with previously active IP Security (IPsec) phase-2 tunnels, use the **show crypto mib ipsec flowmib history** command in privileged EXEC mode.

show crypto mib ipsec flowmib history [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following example displays the IPsec phase 2 history statistics for all VRFs:

```
Router# show crypto mib ipsec flowmib history

vrf Global
  Reason:                       Operation request
  Index:                        1
  Local address:                192.1.2.1
  Remote address:               192.1.2.2
  IPSEC keying:                 IKE
  Encapsulation mode:           1
  Lifetime (KB):                4608000
  Lifetime (Sec):               3600
  Active time:                  00:24:32
  Lifetime threshold (KB):      423559168
  Lifetime threshold (Sec):     3590000
  Total number of refreshes:    0
  Expired SA instances:         4
  Current SA instances:         4
  In SA DH group:               1
  In sa encrypt algorithm       des
  In SA auth algorithm:         rsig
  In SA ESP auth algo:          ESP_HMAC_SHA
  In SA uncompress algorithm:   None
  Out SA DH group:              1
  Out SA encryption algorithm:  des
  Out SA auth algorithm:        ESP_HMAC_SHA
  Out SA ESP auth algorithm:    ESP_HMAC_SHA
  Out SA uncompress algorithm:  None
  In octets:                    400
  Decompressed octets:          400
  In packets:                   4
  In drops:                         0
  In replay drops:                  0
  In authentications:               4
```

```
In authentication failures:      0
In decrypts:                     4
In decrypt failures:             0
Out octets:                      704
Out uncompressed octets:         704
Out packets:                     4
Out drops:                       1
Out authentications:             4
Out authentication failures:     0
Out encryptions:                 4
Out encryption failures:         0
Compressed octets:               0
Decompressed octets:             0
Out uncompressed octets:         704
```

Table 113 describes the significant fields shown in the display.

Table 113 show crypto mib ipsec flowmib history Field Descriptions

Field	Description
Reason	The reason the IPsec phase-2 tunnel was terminated, which are: • 1—All other reasons. • 2—The tunnel terminated normally. • 3—The operator requested the tunnel termination. • 4—A peer delete request was received. • 5—The contact with peer was lost. • 6—A local failure occurred. • 7—The operator initiated a check point request.
Index	The index of the IPsec phase-2 tunnel history table. The value of the index is an integer that begins at one and is incremented with each tunnel that ends. The index value will wrap at 2,147,483,647.
IPSEC keying	The type of key used by the IPsec phase-2 tunnel.
Total number of refreshes	The total number of SA refreshes performed.
In octets	The total number of octets received by the IPsec phase-2 tunnel. The value is accumulated before determining whether or not the packet should be decompressed.
In drops	The total number of packets dropped during receive processing by this IPsec phase-2 tunnel. The number of drops does not include packets dropped due to anti-replay processing.
In replay drops	The total number of packets dropped during receive processing due to anti-replay processing by the IPsec phase-2 tunnel.

Related Commands

Command	Description
show crypto mib ipsec flowmib endpoint	Displays IPsec phase-2 tunnel endpoint table.
show crypto mib ipsec flowmib failure	Displays statistics associated with IPsec phase-2 failure.
show crypto mib ipsec flowmib global	Displays IPsec phase-2 global statistics.
show crypto mib ipsec flowmib spi	Displays the IPsec phase-2 SPI table.
show crypto mib ipsec flowmib tunnel	Displays statistics for all active IPsec phase-2 tunnels.

show crypto mib ipsec flowmib history failure size

To display the size of the IP Security (IPSec) failure history table, use the **show crypto mib ipsec flowmib history failure size** command in privileged EXEC mode.

show crypto mib ipsec flowmib history failure size

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(4)E	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show crypto mib ipsec flowmib history failure size** command to display the size of the failure history table.

Examples

The following is sample output from the **show crypto mib ipsec flowmib history failure size** command:

```
Router# show crypto mib ipsec flowmib history failure size

IPSec Failure Window size: 140
```

Related Commands

Command	Description
crypto mib ipsec flowmib history failure size	Changes the size of the IPSec failure history table.
show crypto mib ipsec flowmib version	Displays the IPSec Flow MIB version used by the router.

show crypto mib ipsec flowmib history tunnel size

To display the size of the IP Security (IPSec) tunnel history table, use the **show crypto mib ipsec flowmib history tunnel size** command in privileged EXEC mode.

show crypto mib ipsec flowmib history tunnel size

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(4)E	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show crypto mib ipsec flowmib history tunnel size** command to display the size of the tunnel history table.

Examples

The following is sample output from the **show crypto mib ipsec flowmib history tunnel size** command:

```
Router# show crypto mib ipsec flowmib history tunnel size

IPSec History Window Size: 130
```

Related Commands

Command	Description
crypto mib ipsec flowmib history tunnel size	Changes the size of the IPSec tunnel history table.
show crypto mib ipsec flowmib version	Displays the IPSec Flow MIB version used by the router.

show crypto mib ipsec flowmib spi

To display the IP Security (IPsec) phase-2 security protection index (SPI) table, use the **show crypto mib ipsec flowmib spi** command in privileged EXEC mode.

show crypto mib ipsec flowmib spi [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

The IPsec phase-2 SPI table contains an entry for each active and expiring security association (SA).

Examples

The following example displays the IPsec phase-2 SPI table for all VRFs:

```
Router# show crypto mib ipsec flowmib spi

vrf Global
 Tunnel Index:          1
  SPI Index:            1
  SPI Value:            0xCC57D053
  SPI Direction:        In
  SPI Protocol:         AH
  SPI Status:           Active

  SPI Index:            2
  SPI Value:            0x68612DF
  SPI Direction:        Out
  SPI Protocol:         AH
  SPI Status:           Active

  SPI Index:            3
  SPI Value:            0x56947526
  SPI Direction:        In
  SPI Protocol:         ESP
  SPI Status:           Active

  SPI Index:            4
  SPI Value:            0x8D7C2204
  SPI Direction:        Out
  SPI Protocol:         ESP
  SPI Status:           Active
```

The field descriptions in the display are self-explanatory.

Related Commands

Command	Description
show crypto mib ipsec flowmib endpoint	Displays IPsec phase-2 tunnel endpoint table.
show crypto mib ipsec flowmib failure	Displays statistics associated with IPsec phase-2 failure.
show crypto mib ipsec flowmib global	Displays IPsec phase-2 global statistics.
show crypto mib ipsec flowmib history	Displays statistics associated with previously active IPsec phase-2 tunnels.
show crypto mib ipsec flowmib tunnel	Displays statistics for all active IPsec phase-2 tunnels.

show crypto mib ipsec flowmib tunnel

To display statistics for all active IP Security (IPsec) phase-2 tunnels, use the **show crypto mib ipsec flowmib tunnel** command in privileged EXEC mode.

show crypto mib ipsec flowmib tunnel [**index** *tunnel-mib-index*] [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.
index *tunnel-mib-index*	(Optional) Displays tunnel MIB information for the specified active tunnel. The tunnel MIB index is an integer, 0–65535.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following example displays statistics for all active IPsec phase-2 tunnels for all tunnel indexes and VRFs:

```
Router# show crypto mib ipsec flowmib tunnel

vrf Global
  Index:                            1
  Local address:                    192.0.2.1
  Remote address:                   192.0.2.2
  IPSEC keying:                     IKE
  Encapsulation mode:               1
  Lifetime (KB):                    4608000
  Lifetime (Sec):                   3600
  Active time:                      00:05:46
  Lifetime threshold (KB):          64
  Lifetime threshold (Sec):         10
  Total number of refreshes:        0
  Expired SA instances:             0
  Current SA instances:             4
  In SA DH group:                   1
  In sa encrypt algorithm:          des
  In SA auth algorithm:             rsig
  In SA ESP auth algo:              ESP_HMAC_SHA
  In SA uncompress algorithm:       None
  Out SA DH group:                  1
  Out SA encryption algorithm:      des
  Out SA auth algorithm:            ESP_HMAC_SHA
  Out SA ESP auth algorithm:        ESP_HMAC_SHA
  Out SA uncompress algorithm:      None
  In octets:                           400
```

```
Decompressed octets:                  400
In packets:                           4
In drops:                             0
In replay drops:                      0
In authentications:                   4
In authentication failures:           0
In decrypts:                          4
In decrypt failures:                  0
Out octets:                           704
Out uncompressed octets:              704
Out packets:                          4
Out drops:                            1
Out authentications:                  4
Out authentication failures:          0
Out encryptions:                      4
Out encryption failures:              0
Compressed octets:                    0
Decompressed octets:                  0
Out uncompressed octets:              704
```

Table 114 describes the significant fields shown in the display.

Table 114 show crypto mib ipsec flowmib tunnel Field Descriptions

Field	Description
Index	The index of the IPsec phase-2 tunnel table. The index value is an integer that begins at one and is incremented with each tunnel that is created. The index value will wrap at 2,147,483,647.
Total number of refreshes	The total number of SA refreshes performed.
Current SA instances	The number of SA instances that are currently active or expiring.
In octets	The total number of octets received by the IPsec phase-2 tunnel. This total number is accumulated before determining whether or not the packet should be decompressed.
Decompressed octets	The total number of decompressed octets received by the IPsec phase-2 tunnel. The total number is accumulated after the packet is decompressed. If compression is not being used, the total number will match the value of cipSecTunInOctets.
In drops	The total number of packets dropped during receive processing by the IPsec phase-2 tunnel. This count does not include packets dropped due to anti-replay processing.
In replay drops	The total number of packets dropped during receive processing due to anti-replay processing by the IPsec phase-2 tunnel.
Out octets	The total number of octets sent by the IPsec phase-2 tunnel. This value is accumulated after determining whether or not the packet should be compressed.

Related Commands

Command	Description
show crypto mib ipsec flowmib endpoint	Displays IPsec phase-2 tunnel endpoint table.
show crypto mib ipsec flowmib failure	Displays statistics associated with IPsec phase-2 failure.
show crypto mib ipsec flowmib global	Displays IPsec phase-2 global statistics.
show crypto mib ipsec flowmib history	Displays statistics associated with previously active IPsec phase-2 tunnels.
show crypto mib ipsec flowmib spi	Displays the IPsec phase-2 SPI table.

show crypto mib ipsec flowmib version

To display the IP Security (IPSec) MIB version used by the router, use the **show crypto mib ipsec flowmib version** command in privileged EXEC mode.

show crypto mib ipsec flowmib version

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(4)E	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show crypto mib ipsec flowmib version** command to display the MIB version used by the management applications to identify the feature set.

Note The MIB version can also be obtained by querying the MIB element cipSecMibLevel using Simple Network Management Protocol (SNMP).

Examples

The following is sample output from the **show crypto mib ipsec flowmib version** command:

```
Router# show crypto mib ipsec flowmib version

IPSec Flow MIB version: 1
```

Related Commands

Command	Description
show crypto mib ipsec flowmib history failure size	Displays the size of the IPSec failure history table.
show crypto mib ipsec flowmib history tunnel size	Displays the size of the IPSec tunnel history table.

show crypto mib isakmp flowmib failure

To display the statistics associated with an Internet Security Association and Key Management Protocol (ISAKMP) phase-1 failure, use the **show crypto mib isakmp flowmib failure** command in privileged EXEC mode.

show crypto mib isakmp flowmib failure [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for a specific Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following is sample output from the **show crypto mib isakmp flowmib failure** command:

```
vrf Global
 Index:                       1
 Reason:                      peer lost
 Failure time since reset:    00:07:27
 Local type:                  ID_IPV4_ADDR
 Local value:                192.0.2.1
 Remote type:                 ID_IPV4_ADDR
 Remote Value:                192.0.2.2
 Local Address:               192.0.2.1
 Remote Address:              192.0.2.2
 Index:                       2
 Reason:                      peer lost
 Failure time since reset:    00:07:27
 Local type:                  ID_IPV4_ADDR
 Local value:                192.0.3.1
 Remote type:                 ID_IPV4_ADDR
 Remote Value:                192.0.3.2
 Local Address:               192.0.3.1
 Remote Address:              192.0.3.2
 Index:                       3
 Reason:                      peer lost
 Failure time since reset:    00:07:32
 Local type:                  ID_IPV4_ADDR
 Remote type:                 ID_IPV4_ADDR
 Remote Value:                192.0.2.2
 Local Address:               192.0.2.1
 Remote Address:              192.0.2.2
```

Table 115 describes the significant fields shown in the display.

Table 115 show crypto mib isakmp flowmib failure Field Descriptions

Field	Description
Index	The IPsec phase-1 failure table index. The value of the index is a number that begins at one and is incremented with each IPsec phase-1 failure. The index value will wrap at 2,147,483,647.
Reason	The reason for the failure, which include: • 1—All other reasons. • 2—A peer delete request was received. • 3—The contact with peer was lost. • 4—A local failure occurred. • 5—An authentication failure occurred. • 6—A hash validation failure occurred. • 7—An encryption failure occurred. • 8—An internal error occurred. • 9—A system capacity failure occurred. • 10—A proposal failure occurred. • 11—The peer certificate was unavailable. • 12—The peer certificate was invalid. • 13—The local certificate expired. • 14—A certificate revoke list (CRL) failure occurred. • 15—A peer encoding error occurred. • 16—The SA did not exist. • 17—The operator requested tunnel termination.
Failure time since reset	The value of sysUpTime in hundredths of seconds at the time of the failure.
Local type	The type of local peer identity. • 1—Indicates an IP address identity type. • 2—Indicates a hostname identity type.
Local value	The value of the local peer identity. If the local peer type is an IP address, then the value is the IP address used to identify the local peer. If the local peer type is a hostname, then the value is the hostname used to identify the local peer.
Remote type	The type of remote peer identity. • 1—Indicates an IP address identity type. • 2—Indicates a hostname identity type.

Table 115 show crypto mib isakmp flowmib failure Field Descriptions (continued)

Field	Description
Remote Value	The value of the remote peer identity. If the remote peer type is an IP address, then the value is the IP address used to identify the remote peer. If the remote peer type is a hostname, then the value is the hostname used to identify the remote peer.
Local Address	The IP address of the local peer.
Remote Address	The IP address of the remote peer.

Related Commands

Command	Description
show crypto ipsec transform-set	Displays configured IPsec transform sets.
show crypto map	Displays IPsec crypto map configurations.
show crypto mib isakmp flowmib global	Displays global ISAKMP statistics.
show crypto mib isakmp flowmib history	Displays statistics associated with previously active ISAKMP tunnels.
show crypto mib isakmp flowmib peer	Displays attributes for an ISKMP peer association.
show crypto mib isakmp flowmib tunnel	Displays statistics associated with active ISAKMP tunnels.

show crypto mib isakmp flowmib global

To display the global Internet Security Association and Key Management Protocol (ISAKMP) phase-1 statistics, use the **show crypto mib isakmp flowmib global** command in privileged EXEC mode.

show crypto mib isakmp flowmib global [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for a specific Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following example displays global ISAKMP statistics:

```
Router# show crypto mib isakmp flowmib global

vrf Global
  Active Tunnels:                       3
  Previous Tunnels:                     0
  In octets:                            2856
  Out octets:                           3396
  In packets:                           16
  Out packets:                          19
  In packets drop:                      0
  Out packets drop:                     0
  In notifys:                           4
  Out notifys:                          7
  In P2 exchg:                          3
  Out P2 exchg:                         6
  In P2 exchg invalids:                 0
  Out P2 exchg invalids:                0
  In P2 exchg rejects:                  0
  Out P2 exchg rejects:                 0
  In IPSEC delete:                      0
  Out IPSEC delete:                     0
  SAs locally initiated:                3
  SAs locally initiated failed:         0
  SAs remotely initiated failed:        0
  System capacity failures:             0
  Authentication failures:              0
  Decrypt failures:                     0
  Hash failures:                        0
  Invalid SPI:                          0
```

Table 116 describes the fields shown in the display.

Table 116 show crypto mib isakmp flowmib global Field Descriptions

Field	Description
Active Tunnels	The number of currently active IPsec phase-1 IKE tunnels.
Previous Tunnels	The total number of previously active IPsec phase-1 IKE tunnels.
In octets	The total number of octets received by all currently and previously active IPsec phase-1 IKE tunnels.
Out octets	The total number of octets sent by all currently and previously active and IPsec phase-1 IKE tunnels.
In packets	The total number of packets received by all currently and previously active IPsec phase-1 IKE tunnels.
Out packets	The total number of packets sent by all currently and previously active and IPsec phase-1 tunnels.
In packets drop	The total number of packets that were dropped during receive processing by all currently and previously active IPsec phase-1 IKE tunnels.
Out packets drop	The total number of packets that were dropped during send processing by all currently and previously active IPsec phase-1 IKE tunnels.
In notifys	The total number of notifications received by all currently and previously active IPsec phase-1 IKE tunnels.
Out notifys	The total number of notifications sent by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 exchg	The total number of IPsec phase-2 exchanges received by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 exchg	The total number of IPsec phase-2 exchanges that were sent by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 exchg invalids	The total number of IPsec phase-2 exchanges that were received and found to be invalid by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 exchg invalids	The total number of IPsec phase-2 exchanges that were sent and found to be invalid by all currently and previously active IPsec phase-1 tunnels.
In P2 exchg rejects	The total number of IPsec phase-2 exchanges that were received and rejected by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 exchg rejects	The total number of IPsec phase-2 exchanges that were sent and rejected by all currently and previously active IPsec phase-1 IKE tunnels.
In IPSEC delete	The total number of IPsec phase-2 SA delete requests received by all currently and previously active and IPsec phase-1 IKE tunnels.

Table 116 show crypto mib isakmp flowmib global Field Descriptions (continued)

Field	Description
Out IPSEC delete	The total number of IPsec phase-2 SA delete requests sent by all currently and previously active IPsec phase-1 IKE tunnels.
SAs locally initiated	The total number of IPsec phase-1 IKE tunnels that were locally initiated.
SAs locally initiated failed	The total number of IPsec phase-1 IKE tunnels that were locally initiated and failed to activate.
SAs remotely initiated failed	The total number of IPsec phase-1 IKE tunnels that were remotely initiated and failed to activate.
System capacity failures	The total number of system capacity failures that occurred during processing of all current and previously active IPsec phase-1 IKE tunnels.
Authentication failures	The total number of authentications that ended in failure by all current and previous IPsec phase-1 IKE tunnels.
Decrypt failures	The total number of decryptions that ended in failure by all current and previous IPsec phase-1 IKE tunnels.
Hash failures	The total number of hash validations that ended in failure by all current and previous IPsec phase-1 IKE tunnels.
Invalid SPI	The total number of non-existent SAs in failures which occurred during processing of all current and previous IPsec phase-1 IKE tunnels.

Related Commands

Command	Description
show crypto mib isakmp flowmib failure	Displays statistics associated with an ISAKMP failure.
show crypto mib isakmp flowmib history	Displays statistics associated with previously active ISAKMP tunnels.
show crypto mib isakmp flowmib peer	Displays attributes for an ISKMP peer association.
show crypto mib isakmp flowmib tunnel	Displays statistics associated with active ISAKMP tunnels.

show crypto mib isakmp flowmib history

To display the statistics associated with previously active Internet Security Association and Key Management Protocol (ISAKMP) phase-1 tunnels, use the **show crypto mib isakmp flowmib history** command in privileged EXEC mode.

show crypto mib isakmp flowmib history [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for a specific Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following example displays previous ISAKMP phase-1 tunnel information for all VRFs:

```
Router# show crypto mib isakmp flowmib history

vrf Global
  Reason:                          peer lost
  Index:                           2
  Local type:                      ID_IPV4_ADDR
  Local address:                   192.0.2.1
  Remote type:                     ID_IPV4_ADDR
  Remote address:                  192.0.2.2
  Negotiation mode:                Main Mode
  Diffie Hellman Grp:              2
  Encryption algo:                 des
  Hash algo:                       sha
  Auth method:                     psk
  Lifetime:                        86400
  Active time:                     00:06:30
  Policy priority:                 1
  Keepalive enabled:               Yes
  In octets:                       3024
  In packets:                      22
  In drops:                        0
  In notifys:                      18
  In P2 exchanges:                 1
  In P2 exchg invalids:            0
  In P2 exchg rejected:              0
  In P2 SA delete reqs:              0
  Out octets:                        4188
  Out packets:                       33
  Out drops:                         0
  Out notifys:                       28
  Out P2 exchgs:                     2
```

```
Out P2 exchg invalids:              0
Out P2 exchg rejects:               0
Out P2 Sa delete requests:          0
Reason:                             peer lost
Index:                              3
Local type:                         ID_IPV4_ADDR
Local address:                      192.0.3.1
Remote type:                        ID_IPV4_ADDR
Remote address:                     192.0.3.2
Negotiation mode:                   Main Mode
Diffie Hellman Grp:                 2
Encryption algo:                    des
Hash algo:                          sha
Auth method:                        psk
Lifetime:                           86400
Active time:                        00:06:25
Policy priority:                    1
Keepalive enabled:                  Yes
In octets:                          3140
In packets:                         23
In drops:                           0
In notifys:                         19
In P2 exchanges:                    1
In P2 exchg invalids:               0
In P2 exchg rejected:               0
In P2 SA delete reqs:               0
Out octets:                         4304
Out packets:                        34
Out drops:                          0
Out notifys:                        29
Out P2 exchgs:                      2
Out P2 exchg invalids:              0
Out P2 exchg rejects:               0
Out P2 Sa delete requests:          0
```

Table 117 describes the significant fields shown in the display.

Table 117 show crypto mib isakmp flowmib history Field Descriptions

Field	Description
Reason	The reason the IPsec phase-1 IKE tunnel was terminated, which include: • 1—All other reasons. • 2—The tunnel terminated normally. • 3—The operator requested tunnel termination. • 4—A peer delete request was received. • 5—The contact with peer was lost. • 6—A local failure occurred. • 7—The operator initiated a check point request.
Index	The index of the IPsec phase-1 IKE tunnel history table. The value of the index is a number that begins at one and is incremented with each tunnel that ends. The value of this object will wrap at 2,147,483,647.

Table 117 show crypto mib isakmp flowmib history Field Descriptions (continued)

Field	Description
Local type	The type of local peer identity. • 1—Indicates an IP address identity type. • 2—Indicates a hostname identity type.
Local address	The value of the local peer identity. If the local peer type is an IP address, then the value is the IP address used to identify the local peer. If the local peer type is a hostname, then the value is the hostname used to identify the local peer.
Remote type	The type of remote peer identity. • 1—Indicates an IP address identity type. • 2—Indicates a hostname identity type.
Remote address	The value of the remote peer identity. If the remote peer type is an IP address, then the value is the IP address used to identify the remote peer. If the remote peer type is a hostname, then the value is the hostname used to identify the remote peer.
Lifetime	The negotiated lifetime of the IPsec phase-1 IKE tunnel in seconds.
Active time	The length of time the IPsec phase-1 IKE tunnel has been active in hundredths of seconds.
In octets	The total number of octets received by all currently and previously active IPsec phase-1 IKE tunnels.
In packets	The total number of packets received by all currently and previously active IPsec phase-1 IKE tunnels.
In drops	The total number of packets that were dropped during receive processing by all currently and previously active IPsec phase-1 IKE tunnels.
In notifys	The total number of notifications received by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 exchanges	The total number of IPsec phase-2 exchanges received by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 exchg invalids	The total number of IPsec phase-2 exchanges that were received and found to be invalid by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 exchg rejected	The total number of IPsec phase-2 exchanges that were received and rejected by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 SA delete reqs	The total number of IPsec phase-2 SA delete requests received by all currently and previously active and IPsec phase-1 IKE tunnels.
Out octets	The total number of octets sent by all currently and previously active and IPsec phase-1 IKE tunnels.

Table 117 show crypto mib isakmp flowmib history Field Descriptions (continued)

Field	Description
Out packets	The total number of packets sent by all currently and previously active and IPsec phase-1 tunnels.
Out drops	The total number of packets that were dropped during send processing by all currently and previously active IPsec phase-1 IKE tunnels.
Out notifys	The total number of notifications sent by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 exchgs	The total number of IPsec phase-2 exchanges that were sent by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 exchg invalids	The total number of IPsec phase-2 exchanges that were sent and found to be invalid by all currently and previously active IPsec phase-1 tunnels.
Out P2 exchg rejects	The total number of IPsec phase-2 exchanges that were sent and rejected by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 Sa delete requests	The total number of IPsec phase-2 SA delete requests sent by all currently and previously active IPsec phase-1 IKE tunnels.

Related Commands

Command	Description
show crypto mib isakmp flowmib failure	Displays statistics associated with an ISAKMP failure.
show crypto mib isakmp flowmib global	Displays global ISAKMP statistics.
show crypto mib isakmp flowmib peer	Displays attributes for an ISKMP peer association.
show crypto mib isakmp flowmib tunnel	Displays statistics associated with active ISAKMP tunnels.

show crypto mib isakmp flowmib peer

To display attributes for an active Internet Security Association and Key Management Protocol (ISAKMP) phase-1 peer association, use the **show crypto mib isakmp flowmib peer** command in privileged EXEC mode.

show crypto mib isakmp flowmib peer [**index** *peer-mib-index*] [**vrf** *vrf-name*]

Syntax Description

index *peer-mib-index*	(Optional) Displays MIB information for the specified peer. The peer MIB index is an integer, 0–65535.
vrf *vrf-name*	(Optional) Displays the parameters for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following example displays ISAKMP peer information for all indexes and VRFs:

```
Router# show crypto mib isakmp flowmib peer

 vrf Global
  Index:              1
  Local type:         ID_IPV4_ADDR
  Local address:      192.0.2.1
  Remote type:        ID_IPV4_ADDR
  Remote address:     192.0.2.2

  Index:              2
  Local type:         ID_IPV4_ADDR
  Local address:      192.0.3.1
  Remote type:        ID_IPV4_ADDR
  Remote address:     192.0.3.1

  Index:              3
  Local type:         ID_IPV4_ADDR
  Local address:      192.0.4.1
  Remote type:        ID_IPV4_ADDR
  Remote address:     192.0.4.1
```

Table 118 describes the significant fields shown in the display.

Table 118 show crypto mib isakmp flowmib peer Field Descriptions

Field	Description
Index	The index of the active IPsec phase-1 IKE tunnel for this peer association. If an IPsec phase-1 IKE tunnel is not currently active, then the value of this object will be zero.
Local type	The type of local peer identity. • 1—Indicates an IP address identity type. • 2—Indicates a hostname identity type.
Local address	The IP address of the local peer.
Remote type	The type of remote peer identity. • 1—Indicates an IP address identity type. • 2—Indicates a hostname identity type.
Remote address	The IP address of the remote peer.

Related Commands

Command	Description
show crypto mib isakmp flowmib failure	Displays statistics associated with an ISAKMP failure.
show crypto mib isakmp flowmib global	Displays global ISAKMP statistics.
show crypto mib isakmp flowmib history	Displays statistics associated with previously active ISAKMP tunnels.
show crypto mib isakmp flowmib tunnel	Displays statistics associated with active ISAKMP tunnels.

show crypto mib isakmp flowmib tunnel

To display statistics associated with active Internet Security Association and Key Management Protocol (ISAKMP) phase-1 tunnels, use the **show crypto mib isakmp flowmib tunnel** command in privileged EXEC mode.

show crypto mib isakmp flowmib tunnel [**index** *tunnel-mib-index*] [**vrf** *vrf-name*]

Syntax Description

index *tunnel-mib-index*	(Optional) Displays tunnel MIB information for the specified tunnel. The tunnel MIB index is an integer, 0–65535.
vrf *vrf-name*	(Optional) Displays the parameters for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following example displays ISAKMP tunnel information for all indexes and VRFs:

```
Router# show crypto mib isakmp flowmib tunnel

vrf Global
  Index:                    1
  Local type:               ID_IPV4_ADDR
  Local address:            192.0.2.1
  Remote type:              ID_IPV4_ADDR
  Remote address:           192.0.2.2
  Negotiation mode:         Main Mode
  Diffie Hellman Grp:       2
  Encryption algo:          des
  Hash algo:                sha
  Auth method:              psk
  Lifetime:                 86400
  Active time:              00:03:08
  Policy priority:          1
  Keepalive enabled:        Yes
  In octets:                2148
  In packets:               15
  In drops:                 0
  In notifys:               11
  In P2 exchanges:          1
  In P2 exchg invalids:     0
  In P2 exchg rejected:     0
  In P2 SA delete reqs:     0
  Out octets:               2328
  Out packets:              16
  Out drops:                    0
```

```
Out notifys:                    12
Out P2 exchgs:                  2

Out P2 exchg invalids:          0
Out P2 exchg rejects:           0
Out P2 Sa delete requests:      0
```

Table 119 describes the significant fields shown in the display.

Table 119 show crypto mib isakmp flowmib tunnel Field Descriptions

Field	Description
Index	The index of the IPsec phase-1 IKE tunnel table. The value of the index is a number that begins at one and is incremented with each tunnel that is created. The value of this object will wrap at 2,147,483,647.
Local type	The type of local peer identity. • 1—Indicates an IP address identity type. • 2—Indicates a hostname identity type.
Local address	The value of the local peer identity. If the local peer type is an IP address, then the local address is the IP address used to identify the local peer. If the local peer type is a hostname, then the local address is the hostname used to identify the local peer.
Remote type	The type of remote peer identity. • 1—Indicates an IP address identity type. • 2—Indicates a hostname identity type.
Remote address	The value of the remote peer identity. If the remote peer type is an IP address, then the remote address is the IP address used to identify the remote peer. If the remote peer type is a hostname, then the remote address is the hostname used to identify the remote peer.
Negotiation mode	The negotiation mode of the IPsec phase-1 IKE tunnel.
Diffie Hellman Grp	The Diffie Hellman group used in IPsec phase-1 IKE negotiations.
Encryption algo	The encryption algorithm used in IPsec phase-1 IKE negotiations.
Hash algo	The hash algorithm used in IPsec phase-1 IKE negotiations.
Auth method	The authentication method used in IPsec phase-1 IKE negotiations.
Lifetime	The negotiated lifetime of the IPsec phase-1 IKE tunnel in seconds
Active time	The length of time the IPsec phase-1 IKE tunnel has been active in hundredths of seconds.
In octets	The total number of octets received by all currently and previously active IPsec phase-1 IKE tunnels.

Table 119 show crypto mib isakmp flowmib tunnel Field Descriptions (continued)

Field	Description
In packets	The total number of packets received by all currently and previously active IPsec phase-1 IKE tunnels.
In drops	The total number of packets that were dropped during receive processing by all currently and previously active IPsec phase-1 IKE tunnels.
In notifys	The total number of notifications received by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 exchanges	The total number of IPsec phase-2 exchanges received by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 exchg invalids	The total number of IPsec phase-2 exchanges that were received and found to be invalid by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 exchg rejected	The total number of IPsec phase-2 exchanges that were received and rejected by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 SA delete reqs	The total number of IPsec phase-2 SA delete requests received by all currently and previously active and IPsec phase-1 IKE tunnels.
Out octets	The total number of octets sent by all currently and previously active and IPsec phase-1 IKE tunnels.
Out packets	The total number of packets sent by all currently and previously active and IPsec phase-1 tunnels.
Out drops	The total number of packets that were dropped during send processing by all currently and previously active IPsec phase-1 IKE tunnels.
Out notifys	The total number of notifications sent by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 exchgs	The total number of IPsec phase-2 exchanges that were sent by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 exchg invalids	The total number of IPsec phase-2 exchanges that were sent and found to be invalid by all currently and previously active IPsec phase-1 tunnels.
Out P2 exchg rejects	The total number of IPsec phase-2 exchanges that were sent and rejected by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 Sa delete requests	The total number of IPsec phase-2 SA delete requests sent by all currently and previously active IPsec phase-1 IKE tunnels.

Related Commands

Command	Description
show crypto mib isakmp flowmib failure	Displays statistics associated with an ISAKMP failure.
show crypto mib isakmp flowmib global	Displays global ISAKMP statistics.
show crypto mib isakmp flowmib history	Displays statistics associated with previously active ISAKMP tunnels.
show crypto mib isakmp flowmib peer	Displays attributes for an ISKMP peer association.

show crypto pki benchmarks

To display benchmarking data for Public Key Infrastructure (PKI) performance monitoring and optimization that was collected, use the **show crypto pki benchmarks** command in privileged EXEC mode.

show crypto pki benchmarks [**failures**]

Syntax Description

failures	(Optional) Includes validation failures only.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Use the **show crypto pki benchmarks** command to display benchmarking data for PKI performance monitoring and optimization that was collected.

The IOS PKI Performance Monitoring and Optimization feature enables you to collect the following types of PKI performance data:

- Time to validate entire certificate chain.
- Time to verify each certificate.
- Time to check revocation status for each certificate.
- Time to fetch certificate revocation list (CRL) database for each fetch location.
- Time to fetch Simple Certificate Enrollment Protocol (SCEP) method capabilities to retrieve the CRL.
- Time to process each CRL.
- Time to process the Online Certificate Status Protocol (OCSP) response. OCSP is a certificate revocation mechanism.
- Time to fetch Authentication, Authorization, and Accounting (AAA).
- CRL size.
- Validation result.
- Validation Bypass (pubkey cached).
- Method used to fetch a CRL.
- PKI session identifier.
- Crypto engine used (hardware, software, etoken).

Examples

The following example displays **show crypto pki benchmark** command output of all PKI benchmarking data:

```
Router# show crypto pki benchmark

Display Validation Benchmark Table

 4 Records collected

Validation Session 10006
  Start: 20:47:29.021 GMT Wed Oct 27 2010
  Duration: 756 ms
  Peer Certificate Serial Number (hex): 296ED1EB0000000052FA
  Pubkey Bypass: no
  Result: Success
  Size of Chain to Validate: 1
  Revocation Check for Certificate 1 of 1
    Start: 20:47:29.063 GMT Wed Oct 27 2010
    Duration: 714 ms
  CRL Fetch - http://msca-root/CertEnroll/msca-root.crl
      Start: 20:47:29.067 GMT Wed Oct 27 2010
      Duration: 661 ms
      Fetch Result: Success
  CRL Insert
      Start: 20:47:29.731 GMT Wed Oct 27 2010
      Duration: 24 ms
  CRL Size: 582

Validation Session 10007
  Start: 20:48:15.897 GMT Wed Oct 27 2010
  Duration: 26 ms
  Pubkey Bypass: no
  Result: Failed CRYPTO_CERT_EXPIRED
  Size of Chain to Validate: 1

Validation Session 10008
  Start: 20:49:08.916 GMT Wed Oct 27 2010
  Duration: 26 ms
  Pubkey Bypass: no
  Result: Failed CRYPTO_CERT_EXPIRED
  Size of Chain to Validate: 1

Validation Session 10009
  Start: 20:49:15.051 GMT Wed Oct 27 2010
  Duration: 32 ms
  Peer Certificate Serial Number (hex): 296ED1EB0000000052FA
  Pubkey Bypass: no
  Result: Success
  Size of Chain to Validate: 1
  Revocation Check for Certificate 1 of 1
    Start: 20:49:15.076 GMT Wed Oct 27 2010
    Duration: 6 ms
```

The following example displays **show crypto pki benchmark** command output of a section filter in PKI benchmarking data:

```
Router# show crypto pki benchmark | section Revocation
  Revocation Check for Certificate 1 of 1
    Start: 20:47:29.063 GMT Wed Oct 27 2010
    Duration: 714 ms
  Revocation Check for Certificate 1 of 1
    Start: 20:49:15.076 GMT Wed Oct 27 2010
    Duration: 6 ms
```

Related Commands

Command	Description
clear crypto pki benchmark	Clears PKI benchmarking performance monitoring and optimization data and releases all memory associated with this data.
crypto pki benchmark	Starts or stops benchmarking data for PKI performance monitoring and optimization.

show crypto pki certificates

To display information about your certificate, the certification authority certificate (CA), and any registration authority (RA) certificates, use the **show crypto pki certificates** command in privileged EXEC mode.

show crypto pki certificates [*trustpoint-name* [**verbose**]]

Syntax Description

trustpoint-name	(Optional) Name of the trustpoint. Using this argument indicates that only certificates that are related to the trustpoint are to be displayed.
verbose	(Optional) More detailed information is to be displayed. **Note** The **verbose** keyword can be used only if a trustpoint name is entered.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3 T	The **show crypto ca certificates** command was introduced.
12.2(13)T	The *trustpoint-name* argument was added.
12.3(7)T	This command replaced the **show crypto ca certificates** command.
12.3(8)T	The **verbose** keyword was added.
12.3(14)T	The command output was modified to include persistent self-signed certificate parameters.
12.4(2)T	The command output was modified to include shadow public key infrastructure (PKI), or rollover, certificate details.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(22)T	The command output was modified to include X.509 certificate IP address extension information.

Usage Guidelines

This command shows information about the following certificates:

- Your certificate, if you have requested one from the CA (see the **crypto pki enroll** command)
- The certificate of the CA, if you have received the certificate of the CA (see the **crypto pki authenticate** command)
- RA certificates, if you have received RA certificates (see the **crypto pki authenticate** command)
- A self-signed certificate, if one has been requested
- Shadow PKI, or rollover, certificate details, if one or more shadow PKI certificates exist

Examples

The following is sample output from the **show crypto pki certificates** command after you authenticated the CA by requesting the certificate of the CA and public key with the **crypto pki authenticate** command:

```
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

The CA certificate might show Key Usage as “Not Set.”

The following is sample output from the **show crypto pki certificates** command, and it shows the certificate of the router and the certificate of the CA. In this example, a single, general-purpose Rivest, Shamir, and Adelman (RSA) key pair was previously generated, and a certificate was requested but not received for that key pair.

```
Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
    Serial Number: 04806682
  Status: Pending
  Key Usage: General Purpose
    Fingerprint: 428125BD A3419600 3F6C7831 6CD8FA95 00000000

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

Note that in the previous sample, the certificate status of the router shows “Pending.” After the router receives its certificate from the CA, the Status field changes to “Available” in the **show** output.

The following is sample output from the **show crypto pki certificates** command, and it shows the certificates of two routers and the certificate of the CA. In this example, special-usage RSA key pairs were previously generated, and a certificate was requested and received for each key pair.

```
Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: 428125BDA34196003F6C78316CD8FA95
  Key Usage: Signature

Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: AB352356AFCD0395E333CCFD7CD33897
  Key Usage: Encryption

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

The following is sample output from the **show crypto pki certificates** command when the CA supports an RA. In this example, the CA and RA certificates were previously requested with the **crypto pki authenticate** command.

```
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set

RA Signature Certificate
  Status: Available
  Certificate Serial Number: 34BCF8A0
  Key Usage: Signature

RA KeyEncipher Certificate
  Status: Available
  Certificate Serial Number: 34BCF89F
  Key Usage: Encryption
```

The following is sample output from the **show crypto pki certificates** command using the optional *trustpoint-name* argument and **verbose** keyword. The output shows the certificate of a router and the certificate of the CA. In this example, general-purpose RSA key pairs were previously generated, and a certificate was requested and received for the key pair.

```
Certificate
   Status: Available
   Version: 3
   Certificate Serial Number: 18C1EE03000000004CBD
   Certificate Usage: General Purpose
   Issuer:
     cn=msca-root
     ou=pki msca-root
     o=company
     l=stown
     st=state
     c=US
     ea=user@example.com
   Subject:
     Name: myrouter.example.com
     hostname=myrouter.example.com
   CRL Distribution Points:
     http://msca-root/CertEnroll/msca-root.crl
   Validity Date:
     start date: 19:50:40 GMT Oct 5 2004
     end   date: 20:00:40 GMT Oct 12 2004
   Subject Key Info:
     Public Key Algorithm: rsaEncryption
     RSA Public Key: (360 bit)
   Signature Algorithm: SHA1 with RSA Encryption
   Fingerprint MD5: 2B5F53E6 E3E892E6 3A9D3706 01261F10
   Fingerprint SHA1: 315D127C 3AD34010 40CE7F3A 988BBDA5 CD528824
   X509v3 extensions:
     X509v3 Key Usage: A0000000
       Digital Signature
       Key Encipherment
     X509v3 Subject Key ID: D156E92F 46739CBA DFE66D2D 3559483E B41ECCF4
     X509v3 Authority Key ID: 37F3CC61 AF5E7C0B 434AB364 CF9FA0C1 B17C50D9
     Authority Info Access:
   Associated Trustpoints: msca-root
   Key Label: myrouter.example.com

CA Certificate
   Status: Available
   Version: 3
   Certificate Serial Number: 1244325DE0369880465F977A18F61CA8
   Certificate Usage: Signature
```

```
  Issuer:
    cn=msca-root
    ou=pki msca-root
    o=company
    l=town
    st=state
    c=US
    ea=user@example.com
  Subject:
    cn=msca-root
    ou=pki msca-root
    o=company
    l=town
    st=state
    c=US
    ea=user@example.com
  CRL Distribution Points:
    http://msca-root.example.com/CertEnroll/msca-root.crl
  Validity Date:
    start date: 22:19:29 GMT Oct 31 2002
    end   date: 22:27:27 GMT Oct 31 2017
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (512 bit)
  Signature Algorithm: SHA1 with RSA Encryption
  Fingerprint MD5: 84E470A2 38176CB1 AA0476B9 C0B4F478
  Fingerprint SHA1: 0F57170C 654A5D7D 10973553 EFB0F94F 2FAF9837
  X509v3 extensions:
    X509v3 Key Usage: C6000000
      Digital Signature
      Non Repudiation
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: 37F3CC61 AF5E7C0B 434AB364 CF9FA0C1 B17C50D9
    X509v3 Basic Constraints:
        CA: TRUE
    Authority Info Access:
  Associated Trustpoints: msca-root
```

The following example shows that a self-signed certificate has been created using a user-defined trustpoint:

```
Router Self-Signed Certificate
  Status: Available
  Certificate Serial Number: 01
  Certificate Usage: General Purpose
  Issuer:
    serialNumber=C63EBBE9+ipaddress=10.3.0.18+hostname=test.company.com
  Subject:
    Name: router.company.com
    IP Address: 10.3.0.18
    Serial Number: C63EBBE9
    serialNumber=C63EBBE9+ipaddress=10.3.0.18+hostname=test.company.com
  Validity Date:
    start date: 20:51:40 GMT Nov 29 2004
    end   date: 00:00:00 GMT Jan 1 2020
  Associated Trustpoints: local
```

The following example shows that a shadow CA certificate, or rollover certificate, is available and shows its status:

```
Router# show crypto ca certificates
```

```
 Rollover Certificate

Status: Waiting for rollover
Certificate Serial Number: 3C
Certificate Usage: General Purpose
Issuer:
  cn=ezsdd
Subject:
  Name: Router.company.com
  Serial Number: 3A9BEC55
  serialNumber=3A9BEC55+hostname=Router.company.com
Validity Date:
  start date: 21:22:08 UTC Mar 17 2004
  end   date: 21:22:08 UTC Mar 17 2005
  renew date: 00:00:00 UTC Jan 1 1970
Associated Trustpoints: tti
```

Related Commands

Command	Description
crypto pki authenticate	Authenticates the CA (by obtaining the certificate of the CA).
crypto pki enroll	Obtains the certificates of your router from the CA.
debug crypto pki messages	Displays debug messages for the details of the interaction (message dump) between the CA and the route.
debug crypto pki transactions	Displays debug messages for the trace of interaction (message type) between the CA and the router.

show crypto pki certificates storage

To display the current public key infrastructure (PKI) certificate storage location, use the **show crypto pki certificates storage** command in privileged EXEC mode.

show crypto pki certificates storage

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use the **show crypto pki certificates storage** command to display the current PKI certificate storage location.

Examples

The following is sample output for the **show crypto pki certificates storage** command where the certificates are stored in the certs subdirectory of disk0:

```
Router# show crypto pki certificates storage

Certificates will be stored in disk0:/certs/
```

Related Commands

Command	Description
crypto pki certificate storage	Specifies local storage device for PKI certificates.

show crypto pki counters

To display the public key infrastructure (PKI) counters that are configured on the router, use the **show crypto pki counters** command in privileged EXEC mode.

show crypto pki counters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(13)T	This command was introduced.

Examples

The following example shows the listing of all PKI counters that are configured in a router:

```
Router# show crypto pki counters

PKI Sessions Started: 5
PKI Sessions Ended: 5
PKI Sessions Active: 0
Successful Validations: 1
Failed Validations: 4
Bypassed Validations: 0
Pending Validations: 0
CRLs checked: 3
CRL - fetch attempts: 2
CRL - failed attempts: 0
AAA authorizations: 0
```

Table 120 describes the significant fields shown in the display.

Table 120 show crypto pki counters Field Descriptions

Field	Description
PKI Sessions Started	Number of PKI sessions that are started in a router.
PKI Sessions Ended	Number of PKI sessions that are ended in a router.
PKI Sessions Active	Number of PKI sessions that are actively running in a router.
Successful Validations	Number of successful PKI counter validations in a router.
Failed Validations	Number of failed PKI counter validations in a router.
Bypassed Validations	Number of validations that were bypassed during a PKI counter validation in a router.
Pending Validations	Number of pending PKI counter validations in a router.
CRLs checked	Number of certificate revocation lists (CRLs) that are checked in a PKI session.
CRL - fetch attempts	Number of times a CRL is queried and fetched.

Table 120 show crypto pki counters Field Descriptions

Field	Description
CRL - failed attempts	Number of times failed in querying and fetching a CRL.
AAA authorizations	Number of authentication, authorization, and accounting (AAA) authorizations that were used to create named methods lists in a PKI session.

Related Commands

Command	Description
show crypto pki certificates	Displays information about the certification authority certificate and any RA certificates.
show crypto pki crls	Displays the current CRL on the router.
show crypto pki server	Displays the current state and configuration of the certificate server.
show crypto pki timers	Displays the status of the managed timers that are maintained by Cisco IOS for PKI.
show crypto pki token	Displays the Cisco IOS PKI tokens that are configured on the router.
show crypto pki trustpoints	Displays the Cisco IOS PKI trustpoints that are configured in the router.

show crypto pki crls

To display the current certificate revocation list (CRL) on the router, use the **show crypto pki crls** command in privileged EXEC mode.

show crypto pki crls

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1	The **show crypto ca crls** command was introduced.
12.3(7)T	This command replaced the **show crypto ca crls** command.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.(33)SXH.
12.4(20)T	The output of this command was updated to include information on the CRL cache size if set by the **crypto pki crl cache** command.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following is sample output of the **show crypto pki crls** command:

```
Router# show crypto pki crls

          CRL Issuer Name:
              OU = vpn, O = company, C = us
              LastUpdate: 16:17:34 PST Jan 10 2002
              NextUpdate: 17:17:34 PST Jan 11 2002
              Retrieved from CRL Distribution Point:
                LDAP: CN = CRL1, OU = vpn, O = company, C = us
```

The following is sample output of the **show crypto pki crls** command with the maximum CRL cache size set to 2048 bytes:

```
Router# show crypto pki crls

     CRL Issuer Name:
           cn=ioscs,l=Anytown,c=US
           LastUpdate: 02:53:41 GMT Mar 6 2007
           NextUpdate: 02:53:41 GMT Mar 13 2007
           Retrieved from CRL Distribution Point:
                ** CDP Not Published - Retrieved via SCEP
     CRL DER is 475 bytes
     CRL is stored in parsed CRL cache
     Parsed CRL cache current size is 1705 bytes
     Parsed CRL cache maximum size is 2048 bytes
```

Related Commands

Command	Description
crypto pki crl cache	Sets the maximum amount of volatile memory used to cache CRLs.
crypto pki crl request	Requests that a new CRL be obtained immediately from the CA.

show crypto pki server

To display the current state and configuration of the certificate server, use the **show crypto pki server** command in privileged EXEC mode.

show crypto pki server [*cs-label*]

Syntax Description

cs-label	(Optional) Name of the certificate server. The name must match the name specified through the **crypto pki server** command.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(2)T	The command output was modified to include shadow, or rollover, public key infrastructure (PKI) certificate information.
15.0(1)M	The command output was modified. • To include whether the server is configured for redundancy and whether its state is active or standby or simplex (active, but standby is not up). • To show the high availability (HA) status while the Hot Standby Router Protocol (HSRP) is coming up.

Usage Guidelines

At startup, the certificate server must check the current configuration before issuing any certificates. As it starts up, the certificate server transitions through the states defined in Table 121. Use the **show crypto pki server** command to display the state of the certificate server.

Table 121 Certificate Server Startup State Descriptions

Certificate Server State	Description
configured	The server is available and has generated the certificate server certificates.
storage configuration incomplete	The server is verifying that the configured storage location is available.
waiting for HTTP server	The server is verifying that the HTTP server is running.
waiting for time setting	The server is verifying that the time has been set.

Examples

The following is sample output from the **show crypto pki server** command:

```
Router# show crypto pki server

Certificate Server status: disabled, storage configuration incomplete
    Granting mode is: manual
    Last certificate issued serial number: 0
    CA certificate expiration timer: 21:29:38 GMT Jun 5 2006
    CRL NextUpdate timer: 21:31:39 GMT Jun 6 2003
    Current storage dir: ftp://myftpserver
    Database Level: Minimum - no cert data written to storage
```

Table 122 describes the significant fields shown in the display.

Table 122 show crypto pki server Field Descriptions

Field	Description
Granting mode is	Specifies whether certificate enrollment requests should be granted manually (which is the default) or automatic (through the **grant automatic** command). **Note** The **grant automatic** command should be used *only* when testing and building simple networks. This command *must* be disabled before the network is accessible by the Internet.
Last certificate issued serial number	The serial number of the latest certificate. (To specify the distinguished name (DN) as the certification authority (CA) issuer name, use the **issuer-name** command.)
CA certificate expiration timer	The expiration date for the CA certificate. (To specify the expiration date, use the **lifetime** command.)
CRL NextUpdate timer	The next time the certificate revocation list (CRL) will be updated. (To specify the CRL lifetime, in hours, use the **lifetime crl** command.)
Current storage dir	The location where all database entries for the certificate server will be written out. (To specify a location, use the **database url** command.)
Database Level	The type of data that is stored in the certificate enrollment database—Minumum, names, or complete. (To specify the data type to be stored, use **database level** command.)

The following is sample output from the **show crypto pki server** command when redundancy is configured and its state is simplex:

```
Router# show crypto pki server cert1

Certificate Server cert1:
    Status: disabled
    State: disabled
    Server's configuration is unlocked  (enter "no shut" to lock it)
    Issuer name: CN=cert1
    CA cert fingerprint: -Not found-
    Granting mode is: manual
    Last certificate issued serial number (hex): 0
    CA certificate expiration timer: 00:00:00 UTC Jan 1 1970
    CRL not present.
```

```
    Current primary storage dir: nvram:
    Database Level: Minimum - no cert data written to storage
    Redundancy configured.  Simplex mode.
```

The following is sample output from the **show crypto pki server** command when redundancy is configured and its state is active:

```
Certificate Server HA:
    Status: enabled
    State: enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name: CN=ioscs,L=Santa Cruz,C=US
    CA cert fingerprint: 42308002 188180FC 9265946F FDC68A52
    Granting mode is: auto
    Last certificate issued serial number (hex): 2
    CA certificate expiration timer: 20:22:55 PST Apr 26 2013
    CRL NextUpdate timer: 20:27:46 PST May 11 2010
    Current primary storage dir: nvram:
    Database Level: Complete - all issued certs written as <serialnum>.cer
    Redundancy configured.  This is active.
```

The following is sample output from the **show crypto pki server** command when redundancy is configured and its state is standby:

```
Certificate Server HA:
    Status: enabled
    State: enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name: CN=ioscs,L=Santa Cruz,C=US
    CA cert fingerprint: 42308002 188180FC 9265946F FDC68A52
    Granting mode is: auto
    Last certificate issued serial number (hex): 2
    CA certificate expiration timer: 20:22:55 PST Apr 26 2013
    CRL NextUpdate timer: 20:27:46 PST May 11 2010
    Current primary storage dir: nvram:
    Database Level: Complete - all issued certs written as <serialnum>.cer
    Redundancy configured.  This is standby.
```

The following example shows that the certificate server MyCS has rollover configured. Rollover has not yet occurred. The rollover status “pending” and rollover CA certificate timer show when the rollover timer will be triggered. When this timer is triggered, the shadow certificate will become the active certificate and the previously active certificate will be deleted.

```
Router# show crypto pki server

Certificate Server routercs:
   Status: enabled, configured
   Issuer name: CN=walnutcs
   CA cert fingerprint: 800F5944 74337E5B C2DF6C52 9A7B1BDB
   Granting mode is: auto
   Last certificate issued serial number: 0x6
   CA certificate expiration timer: 22:10:29 GMT Jan 29 2007
   CRL NextUpdate timer: 21:50:56 GMT Mar 5 2004
   Current storage dir: nvram:
   Database Level: Minimum - no cert data written to storage

    Rollover status: pending
    Rollover CA certificate timer: 20:34:23 GMT Jan 8 2005
```

The following example shows that the certificate server MyCS has rollover configured. The rollover time has occurred and the rollover certificate is available. The status shows the rollover certificate fingerprint and rollover CA certificate expiration timer information.

```
Router# show crypto pki server

Certificate Server routercs:
   Status: enabled, configured
   Issuer name: CN=walnutcs
   CA cert fingerprint: 800F5944 74337E5B C2DF6C52 9A7B1BDB
   Granting mode is: auto
   Last certificate issued serial number: 0x7
   CA certificate expiration timer: 22:10:29 GMT Jan 29 2007
   CRL NextUpdate timer: 21:50:56 GMT Mar 5 2004
   Current storage dir: nvram:
   Database Level: Minimum - no cert data written to storage

    Rollover status: available for rollover
    Rollover CA cert fingerprint: 6AAF5944 74227A5B 23DF3E52 9A7F1FEF
    Rollover CA certificate expiration timer: 22:10:29 GMT Jan 29 2017
```

The following example shows a certificate server (CS) that has been prevented from entering rollover state because the Cisco IOS configuration cannot be saved.

```
Router# show crypto pki server

Certificate Server routercs:
   Status: enabled, configured
   Issuer name: CN=walnutcs
   CA cert fingerprint: 800F5944 74337E5B C2DF6C52 9A7B1BDB
   Granting mode is: auto
   Last certificate issued serial number: 0x7
   CA certificate expiration timer: 22:10:29 GMT Jan 29 2007
   CRL NextUpdate timer: 21:50:56 GMT Mar 5 2004
   Current storage dir: nvram:
   Database Level: Minimum - no cert data written to storage

    Rollover status: disabled, unable to save configuration
    Rollover CA cert fingerprint: 6AAF5944 74227A5B 23DF3E52 9A7F1FEF
    Rollover CA certificate expiration timer: 22:10:29 GMT Jan 29 2017
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enter certificate server configuration mode.

show crypto pki server certificates

To display certificate information for all certificates of the specified certificate server, use the **show crypto pki server certificates** command in privileged EXEC mode.

show crypto pki server *cs-label* **certificates** [*start-number* [*end-number*]] [**expired**]

Syntax Description

cs-label	Name of the certificate server. The name must match the name specified via the **crypto pki server** command.
start-number	(Optional) The beginning of the certificate serial number range to display. If only the starting certificate serial number is indicated, information for only the designated certificate is shown if available.
end-number	(Optional) The end of the certificate serial number range to display.
expired	(Optional) Displays the expired certificates.

Command Default

Certificate information is shown for all serial numbers for the specified certificate server, from the first serial number in the certificate database to the last serial number in the certificate database.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

This command displays available information on each certificate for the specified certificate server. If the certificate information is not available, the output displayed reads as "<cert not available>". If the certificate information is incomplete, or if it has been corrupted, the output displayed reads as "<certificate incomplete or corrupted>".

You may display information on all the certificates in the certificate database, one certificate in the certificate database, or a range of certificates in the certificate database by setting the *start-number* and *end-number* arguments.

Examples

The following example shows the listing of all certificates in the certificate database for the certificate server "mycs":

```
Router# show crypto pki server mycs certificates

Serial   Issued date               Expire date               Subject Name
1        02:09:09 PST Jan 22 2007  02:09:09 PST Jan 21 2010  cn=company
2        02:57:59 PST Jan 22 2007  02:57:59 PST Jan 22 2008  hostname=client.example.com
3        03:00:12 PST Jan 22 2007  03:00:12 PST Jan 22 2008  hostname=client.example.com
4        19:53:07 PST Jan 18 2007  19:53:07 PST Jan 19 2007  hostname=client.example.com
5        <cert not available>
6        <cert not available>
7        <cert not available>
```

```
8        02:57:59 PST Jan 22 2007  02:57:59 PST Jan 22 2008  hostname=client.example.com
9        <Certificate incomplete or corrupted>
A        <cert not available>
B        <cert not available>
```

The following example shows the information for certificate serial number 3 in the certificate database for the certificate server “mycs”:

```
Router# show crypto pki server mycs certificates start 3

Serial   Issued date               Expire date               Subject Name
3        03:00:12 PST Jan 22 2007  03:00:12 PST Jan 22 2008  hostname=client.example.com
```

The following example shows the information for certificate serial number 3 through certificate serial number 7 in the certificate database for the certificate server “mycs”:

```
Router# show crypto pki server mycs certificates start 3 end 7

show crypto pki server mycs certificates
Serial   Issued date               Expire date               Subject Name
3        03:00:12 PST Jan 22 2007  03:00:12 PST Jan 22 2008  hostname=client.example.com
4        19:53:07 PST Jan 18 2007  19:53:07 PST Jan 19 2007  hostname=client.example.com
5        <cert not available>
6        <cert not available>
7        <cert not available>
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.
show crypto pki server	Displays the current state and configuration of the certificate server.
show crypto pki server crl	Displays the current status of the CRL.

show crypto pki server crl

To display information regarding the status of the current certificate revocation list (CRL), use the **show crypto pki server crl** command in privileged EXEC mode.

show crypto pki server *cs-label* **crl**

Syntax Description

cs-label	Name of the certificate server. The name must match the name specified via the **crypto pki server** command.

Command Defaults

None.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

CRLs are issued once every specified time period via the **lifetime crl** command. It is the responsibility of the network administrator to ensure that the CRL is available from the location that is specified via the **cdp-url** command. To access information, such as the lifetime and location of the CRL, use the **show crypto pki server crl** command.

Examples

The following example shows how to access CRL information for the certificate server “mycs”:

```
Router# show crypto pki server mycs crl
```

Related Commands

Command	Description
cdp-url	Specifies a CDP to be used in certificates that are issued by the certificate server.
crypto pki server	Enables a Cisco IOS certificate server and enter certificate server configuration mode.
lifetime crl	Defines the lifetime of the CRL that is used by the certificate server.

show crypto pki server requests

To display all outstanding certificate enrollment requests, use the **show crypto pki server requests** command in privileged EXEC mode.

show crypto pki server *cs-label* **requests**

Syntax Description

cs-label	Name of the certificate server. The name must match the name specified via the **crypto pki server** command.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

A certificate enrollment request functions as follows:

- The certificate server receives the enrollment request from an end user, and the following actions occur:
  - A request entry is created in the enrollment request database with the initial state. (See the **show pki server** command for a complete list of certificate enrollment request states.)
  - The certificate server refers to the command-line interface (CLI) configuration (or the default behavior any time a parameter is not specified) to determine the authorization of the request. Thereafter, the state of the enrollment request is updated in the enrollment request database.
- At each Simple Certificate Enrollment Protocol (SCEP) query for a response, the certificate server examines the current request and performs one of the following actions:
  - Responds to the end user with a “pending” or “denied” state.
  - Forwards to the request to the certification authority (CA) core, where it will generate and sign the appropriate certificate, store the certificate in the enrollment request database, and return the request to the built-in certificate server SCEP server, who will reply to the end user with the certificate on the next SCEP request.

If the connection of the client has closed, the certificate server will wait for the client user to request another certificate.

All enrollment requests transitions through the certificate enrollment states that are defined in Table 123.

Table 123 Certificate Enrollment Request State Descriptions

Certificate Enrollment State	Description
authorized	The certificate server has authorized the request.
denied	The certificate server has denied the request for policy reasons.
granted	The CA core has generated the appropriate certificate for the certificate request.
initial	The request has been created by the SCEP server.
malformed	The certificate server has determined that the request is invalid for cryptographic reasons.
pending	The enrollment request must be manually accepted by the network administrator.

Examples

The following example shows output for the certificate server "certsrv1," which has a pending certificate enrollment request:

```
Router# show crypto pki server certsrv1 requests

   Enrollment Request Database:
   ReqID  State      Fingerprint                       SubjectName
   --------------------------------------------------------------
   1      pending    0A71820219260E526D250ECC59857C2D serialNumber=2326115A+hostname=831.
```

The following example shows the output for shadow public key infrastructure (PKI) certificate info requests:

```
Router# show crypto pki server mycs requests

Enrollment Request Database:

RA certificate requests:

  ReqID  State      Fingerprint                       SubjectName

--------------------------------------------------------------
RA rollover certificate requests:

  ReqID  State      Fingerprint                       SubjectName

  --------------------------------------------------------------

Router certificates requests:

  ReqID  State      Fingerprint                       SubjectName

--------------------------------------------------------------

1      pending    A426AF07FE3A4BB69062E0E47198E5BF hostname=client

  Router rollover certificates requests:

  ReqID  State      Fingerprint                       SubjectName

  --------------------------------------------------------------

  2      pending    B69062E0E47198E5BFA426AF07FE3A4B hostname=client
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters PKI configuration mode.

show crypto pki timers

To display the status of the managed timers that are maintained by Cisco IOS for public key infrastructure (PKI), use the **show crypto pki timers** command in privileged EXEC mode.

show crypto pki timers

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	The **show crypto ca timers** command was introduced.
12.3(7)T	This command replaced the **show crypto ca timers** command.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

For each timer, this command displays the time remaining before the timer expires. It also associates trustpoint certification authorities (CAs), except for certificate revocation list (CRL) timers, by displaying the CRL distribution point.

Examples

The following example is sample output for the **show crypto pki timers** command:

```
Router# show crypto pki timers

PKI Timers
| 4d15:13:33.144
 | 4d15:13:33.144  CRL http://msca-root.cisco.com/CertEnroll/msca-root.crl
 |328d11:56:48.372  RENEW msroot
 | 6:43.201  POLL verisign
```

Related Commands

Command	Description
auto-enroll	Enables autoenrollment.
crypto pki trustpoint	Declares the CA that your router should use.

show crypto pki token

To display the Cisco IOS public key infrastructure (PKI) tokens that are configured on the router, use the **show crypto pki token** command in privileged EXEC mode.

show crypto pki token [*name*]

Syntax Description

name	(Optional) Specifies the name of the token.

Command Default

If the *name* argument is not specified, command output is displayed for all PKI tokens.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Examples

The following is sample output from the **show crypto pki token** command:

```
Router# show crypto pki token

Configuration for token usbtoken0:
Automatic login enabled.
Removal timeout 60 seconds

Configuration for token default:
Secondary Config file "BIFT.CFG"
```

Table 124 describes the significant fields shown in the display.

Table 124 show crypto pki token Field Descriptions

Field	Description
Automatic login enabled	Indicates that the crypto PKI token is configured to log in automatically.
Removal timeout 60 seconds	Indicates that the router waits for 60 seconds before removing the Rivest, Shamir, and Adelman (RSA) keys that are stored in the eToken.
Secondary Config file	Indicates that the specified file will be merged with the running configuration after the eToken is logged into the router.

Related Commands

Command	Description
crypto pki token removal timeout	Sets the time interval that the router waits before removing the RSA keys that are stored in the eToken.
crypto pki token secondary config	Merges a specified file with the running configuration after the eToken is logged into the router.

show crypto pki trustpoints

To display the trustpoints that are configured in the router, use the **show crypto pki trustpoints** command in privileged EXEC or user EXEC mode.

show crypto pki trustpoints [**status** | *label* [**status**]]

Syntax Description

status	(Optional) Trustpoint status.
label	(Optional) Trustpoint name.

Command Default

If the *label* argument (trustpoint name) is not specified, command output is displayed for all trustpoints.

Command Modes

Privileged EXEC (#)
User EXEC (>)

Command History

Release	Modification
12.2(8)T	The **show crypto ca trustpoints** command was introduced.
12.3(7)T	This command replaced the **show crypto ca trustpoints** command.
12.3(11)T	The **status** keyword and *label* argument were added.
12.3(14)T	The command output was modified to include persistent self-signed certificate parameters.
12.4(2)T	The command output was modified to include shadow, or rollover, public key infrastructure (PKI) certificate availability and Simple Certificate Enrollment Protocol (SCEP) capabilities.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(22)T	The command output was modified to include X.509 certificate IP address extension information.

Examples

The following is sample output from the **show crypto pki trustpoints** command:

```
Router# show crypto pki trustpoints

Trustpoint bo:
    Subject Name:
    CN = host Certificate Manager
     O = company.com
     C = US
          Serial Number:01
    Certificate configured.
    CEP URL:http://host
    CRL query url:ldap://host
```

The following is sample output from the **show crypto pki trustpoints** command when a persistent self-signed certificate has been configured:

```
Router# show crypto pki trustpoints

Trustpoint local:
    Subject Name:
    serialNumber=C63EBBE9+ipaddress=10.3.0.18+hostname=test.company.com
          Serial Number: 01
    Persistent self-signed certificate trust point
```

The following output shows that a shadow PKI certificate is available and shows the SCEP capabilities:

```
Router# show crypto pki trustpoints

Trustpoint vpn:
   Subject Name:
   cn=Company SSL CA
   o=Company

   Serial Number: 0FFEBBDC1B6F6D9D0EA7875875E4C695

   Certificate configured.

   Rollover certificate configured.
   Enrollment Protocol:
   SCEPv1, PKI Rollover
```

The following output using the **status** keyword shows that the trustpoint is configured in query mode and is currently trying to query the certificates (the certificate authority (CA) certificate and the router certificate are both pending):

```
Router# show crypto pki trustpoints status

Trustpoint yni:
  Issuing CA certificate pending:
    Subject Name:
     cn=r1 Cert Manager,ou=pki,o=company.com,c=country
    Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
  Router certificate pending:
    Subject Name:
     hostname=host.company.com,o=company.com
  Next query attempt:
    52 seconds
```

The following output using the **status** keyword shows that the trustpoint has been authenticated:

```
Router# show crypto pki trustpoints status

Trustpoint yni:
  Issuing CA certificate configured:
    Subject Name:
     cn=r1 Cert Manager,ou=pki,o=company.com,c=country
    Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
  State:
    Keys generated ..... No
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... None
```

The following output using the **status** keyword shows that the trustpoint is enrolling and that two of the certificate requests are pending (Signature and Encryption):

```
Router# show crypto pki trustpoints status

Trustpoint yni:
  Issuing CA certificate configured:
    Subject Name:
     cn=r1 Cert Manager,ou=pki,o=company.com,c=country
    Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
  Router Signature certificate pending:
    Requested Subject Name:
     hostname=host.company.com
    Request Fingerprint: FAE0D74E BB844EA1 54B26698 56AB42EC
    Enrollment polling: 1 times (9 left)
    Next poll: 32 seconds
  Router Encryption certificate pending:
    Requested Subject Name:
     hostname=host.company.com
    Request Fingerprint: F4E815DB D9D9B60F 9B5B1724 3E155DBF
    Enrollment polling: 1 times (9 left)
    Next poll: 44 seconds
  Last enrollment status: Pending
  State:
    Keys generated ..... Yes (Signature, Encryption)
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... Pending
```

The following output using the **status** keyword shows that enrollment has succeeded and that two router certificates have been granted (Signature and Encryption):

```
Router# show crypto pki trustpoints status

Trustpoint yni:
  Issuing CA certificate configured:
    Subject Name:
     cn=r1 Cert Manager,ou=pki,o=company.com,c=country
    Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
  Router Signature certificate configured:
    Subject Name:
     hostname=host.company.com,o=company.com
    Fingerprint: 8A370B8B 3B6A2464 F962178E 8385E9D6
  Router Encryption certificate configured:
    Subject Name:
     hostname=host.company.com,o=company.com
    Fingerprint: 43A03218 C0AFF844 AE0C162A 690B414A
  Last enrollment status: Granted
  State:
    Keys generated ..... Yes (Signature, Encryption)
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... Yes
```

The following output using the **status** keyword shows that trustpoint enrollment has been rejected:

```
Router# show crypto pki trustpoints status

Trustpoint yni:
  Issuing CA certificate configured:
    Subject Name:
     cn=r1 Cert Manager,ou=pki,o=company.com,c=country
    Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
  Last enrollment status: Rejected
  State:
    Keys generated ..... Yes (General Purpose)
```

```
    Issuing CA authenticated ....... Yes
    Certificate request(s) ..... None
```

The following output using the **status** keyword shows that enrollment has succeeded and that the router is configured for autoenrollment using a regenerated key. In addition, the running configuration has been modified so that it will not be saved automatically after autoenrollment.

```
Router# show crypto pki trustpoints status

Trustpoint yni:
  Issuing CA certificate configured:
    Subject Name:
     cn=r1 Cert Manager,ou=pki,o=company.com,c=country
    Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
  Router General Purpose certificate configured:
    Subject Name:
     hostname=host.company.com,o=company.com
    Fingerprint: FC365F95 E24D4B55 81347510 10FFE331
  Last enrollment status: Granted
  Next enrollment attempt:
    01:58:25 PST Feb 14 2004
    * A new key will be generated *
    * Configuration will not be saved after enrollment *
  State:
    Keys generated ..... Yes (General Purpose)
    Issuing CA authenticated ....... Yes
    Certificate request(s) ..... Yes
```

Table 125 describes the significant fields shown in the display.

Table 125 show crypto pki trustpoints Field Descriptions

Field	Description
Trustpoint	Name of the trustpoint.
Issuing CA certificate pending	The CA certificate is being retrieved (query mode).
Issuing CA certificate [not] configured	A CA certificate is [not] configured.
Subject Name	Subject name of the indicated certificate.
Next query attempt	Time until the next query attempt (query mode).
Router certificate pending/Router [key usage] certificate pending	The trustpoint is attempting to obtain the certificate from the CA server (through query mode or enrollment).
Router [key usage] certificate configured	Certificate of the specified key usage is configured.
Requested Subject Name	Subject name used in the enrollment request (Public Key Cryptography Standards 10 [PKCS10]).
Fingerprint MD5/SHA1	Fingerprint of the indicated certificate (Message Digest 5 [MD5] or Secure Hash Algorithm 1 [SHA]1).
Request Fingerprint MD5/SHA1	Fingerprint of the PKCS10 enrollment request (MD5/SHA1).
Enrollment polling: [polled] times ([remaining] left)/Next poll: in seconds	Number of SCEP polling attempts that have been made and that remain before the router gives up/Time until the next polling attempt.
Last enrollment status: Pending/Granted/Rejected/Failed	Last enrollment attempt status (pending, granted, rejected, or failed).

Table 125 show crypto pki trustpoints Field Descriptions (continued)

Field	Description
Next enrollment attempt: *time* (Optional) A new key will be generated. (Optional) Configuration will not be saved after enrollment.	The trustpoint is configured autoenrollment and the autoenrollment will happen at *time*. (Optional) The trustpoint is configured to generate a new key when autoenrollment occurs. (Optional) The running configuration is "dirty," so the configuration will not be saved automatically after autoenrollment.
State	Current state of the trustpoint.
Keys generated	"Yes or No" and the key usage (General Purpose or Signature, Encryption).
Issuing CA authenticated	"Yes or No" if crypto CA authentication has been done successfully.
Certificate request(s)	Progress of current enrollment: "Pending," "Yes," (complete), or "None" (not in progress).

Related Commands

Command	Description
crypto pki trustpoint	Declares the CA that your router should use.

show crypto route

To display routes that are created through IPsec via Reverse Route Injection (RRI) or Easy VPN virtual tunnel interfaces (VTIs) in one table, use the **show crypto route** command in privileged EXEC mode.

show crypto route

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)T	This command was introduced.

Examples

The following example displays routes that were created through IPSec using RRI and VTIs:

```
Router# show crypto route

VPN Routing Table: Shows RRI and VTI created routes
Codes: RRI - Reverse-Route, VTI- Virtual Tunnel Interface
        S - Static Map ACLs

Routes created in table GLOBAL DEFAULT
192.168.6.2/255.255.255.255 [0/0] via 10.0.0.133
                                  on Virtual-Access3 RRI
10.1.1.0/255.255.255.0 [10/0] via Virtual-Access2 VTI
192.168.6.1/255.255.255.255 [0/0] via Virtual-Access2 VTI
```

The fields in the above display are self-explanatory.

Related Commands

Command	Description
reverse-route	Creates source proxy information for a crypto map entry.
set reverse-route	Defines a distance metric for each static route or tags a RRI-created route.

show crypto ruleset

To display information about crypto rules on outgoing packets, use the **show crypto ruleset** command in privileged EXEC mode.

show crypto ruleset [**detail**]

Syntax Description

detail	Displays the directional mode of the IP security (IPsec) security association (SA).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(20)T	This command was introduced.

Examples

The following example displays information about the crypto rules on outgoing packets:

```
Router# show crypto ruleset

Ethernet0/0:
  59 ANY ANY DENY
  11 ANY/848 ANY/848 DENY
 IP ANY ANY IPSec SA Passive
 IP ANY ANY IPSec Cryptomap
```

The following output example shows the directional mode of the IPsec SA:

```
Router# show crypto ruleset detail

Ethernet0/0:
 20000001000019  59 ANY ANY DENY -> 20000001999999
 20000001000029  11 ANY/848 ANY/848 DENY -> 20000001999999
 20000001000035 IP ANY ANY IPSec SA Passive
 20000001000039 IP ANY ANY IPSec Cryptomap
```

Table 126 describes the significant fields shown in the display.

Table 126 show crypto ruleset Field Descriptions

Field	Description
59 ANY ANY DENY	• 59—Hex value of the Open Shortest Path First (OSPF) protocol. • First ANY—Any source IP address. • Second ANY—Any destination IP address. • DENY packets matching this rule will not be encrypted.
11 ANY/848 ANY/848 DENY	• 11—Hex value of the User Datagram Protocol (UDP). • First ANY/848—Any source IP address that has a source port 848. • Second ANY/848—Any destination IP address having a destination port 848. • DENY—Packets matching this rule will not be encrypted.
IP ANY ANY IPSec SA Passive	• Policy of “IP packets with any source or destination address or port” is in IPsec security association (SA) passive mode—Receives both clear and encrypted packets; sends only encrypted packets.
IP ANY ANY IPSec Cryptomap	• Policy of "IP packets with any source or destination address or port" is created by an IPsec crypto map—Receives or sends only encrypted packets.
20000001000019 59 ANY ANY DENY -> 20000001999999	• The first long digit is the priority number of the policy or rule. • The second long digit is the deny priority number of the policy or rule. **Note** These numbers are internal data values and are generally used by developers.

show crypto session

To display status information for active crypto sessions, use the **show crypto session** command in privileged EXEC mode.

show crypto session [**groups** | **interface** *type* [**brief** | **detail**] | **isakmp** [**group** *group-name* | **profile** *profile-name*] [**brief** | **detail**] | [**local** | **remote**] [*ip-address* | *ipv6-address*] [**port** *portnumber*] | [**fvrf** *fvrf-name*] [**ivrf** *ivrf-name*] [**brief** | **detail**] | **summary** *group-name* | **username** *username*]

IPsec and IKE Stateful Failover Syntax

show crypto session [**active** | **standby**]

Syntax Description

groups	(Optional) Displays crypto session group usage for all groups.
interface *type*	(Optional) Displays crypto sessions on the connected interface. • The *type* value is the type of interface connection.
brief	(Optional) Provides brief information about the session, such as the peer IP address, interface, username, group name/phase1 ID, length of session uptime, and current session status (up/down).
detail	(Optional) Provides more detailed information about the session, such as the capability of the Internet Key Exchange (IKE) security association (SA), connection ID, remaining lifetime of the IKE SA, inbound or outbound encrypted or decrypted packet number of the IP security (IPsec) flow, dropped packet number, and kilobyte-per-second lifetime of the IPsec SA.
isakmp group *group-name*	(Optional) Displays crypto sessions using the Internet Security Association and Key Management Protocol (ISAKMP) group. • The *group-name* value is the name of the group.
profile *profile-name*	(Optional) Displays crypto sessions using the ISAKMP profile. • The *profile-name* value is the name of the profile.
local	(Optional) Displays status information about crypto sessions of a local crypto endpoint.
remote	(Optional) Displays status information about crypto sessions of a remote session.
ip-address	IP address of the local or remote crypto endpoint.
ipv6-address	IPv6 address of the local or remote crypto endpoint.
port *portnumber*	(Optional) Port of the local crypto endpoint. • *The portnumber* value can be 1 through 65535. The default value is 500.
fvrf *fvrf-name*	(Optional) Displays status information about the front door virtual routing and forwarding (FVRF) session. • The *fvrf-name* value is the name of the FVRF session.
ivrf *ivrf-name*	(Optional) Displays status information about the inside VRF (IVRF) session. • The *ivrf-name* value is the name of the IVRF session.

summary *group-name*	(Optional) Displays a list of crypto session groups and associated group members.
username *username*	(Optional) Displays the crypto session for the specified extended authentication (XAUTH), public key infrastructure (PKI), or authentication, authorization, and accounting (AAA) username.
active	(Optional) Displays all crypto sessions in the active state.
standby	(Optional) Displays all crypto sessions that are in the standby state.

Command Default

All existing sessions will be displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.3(11)T	This command was modified. The **active** and **standby** keywords were added.
12.4(4)T	This command was modified. IPv6 address information was added to the command output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.4(11)T	This command was modified. The **brief**, **groups**, **interface** *type***, isakmp group** *group-name***, isakmp profile** *profile-name*, **summary**, and **username** *username* keywords and arguments were added. The **show crypto session** output was updated to include username, ISAKMP profile, ISAKMP group, assigned address, and session uptime.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

This command lists all the active Virtual Private Network (VPN) sessions and the IKE and IPsec SAs for each VPN session. The listing will include the following information:

- Interface
- IKE peer description, if available
- IKE SAs that are associated with the peer by which the IPsec SAs are created
- IPsec SAs serving the flows of a session

Multiple IKE or IPsec SAs may be established for the same peer (for the same session), in which case IKE peer descriptions will be repeated with different values for the IKE SAs that are associated with the peer and for the IPsec SAs that are serving the flows of the session.

IPv6 does not support the **fvfr** and **ivrf** keywords and the *vrf-name* argument.

Examples

The following example shows the status information for all active crypto sessions:

```
Router# show crypto session

Crypto session current status

Interface: Virtual-Access2
Username: cisco
Profile: prof
Group: easy
Assigned address: 10.3.3.4
Session status: UP-ACTIVE
Peer: 10.1.1.2 port 500
  IKE SA: local 10.1.1.1/500 remote 10.1.1.2/500 Active
  IKE SA: local 10.1.1.1/500 remote 10.1.1.2/500 Inactive
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 3.3.3.4
        Active SAs: 2, origin: crypto map
```

The following is sample output from the **show crypto session brief** command:

```
Router# show crypto session brief

Status: A- Active, U - Up, D - Down, I - Idle, S - Standby, N - Negotiating
        K - No IKE
ivrf = (none)
           Peer         I/F     Username     Group/Phase1_id    Uptime      Status
           10.1.1.2     Vi2     cisco        easy               00:50:30    UA
```

The following is sample output from the **show crypto session detail** command:

```
Router# show crypto session detail

Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, X - IKE Extended Authentication

Interface: Virtual-Access2
Username: cisco
Profile: prof
Group: easy
Assigned address: 10.3.3.4
Uptime: 00:49:33
Session status: UP-ACTIVE
Peer: 10.1.1.2 port 500 fvrf: (none) ivrf: (none)
Phase1_id: easy
Desc: (none)
IKE SA: local 10.1.1.1/500 remote 10.1.1.2/500 Active
Capabilities:CX connid:1002 lifetime:23:10:15
IPSEC FLOW: permit ip 10.0.0.0/0.0.0.0 host 10.3.3.4
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 0 drop 0 life (KB/Sec) 4425776/626
Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4425776/626
```

Table 127 describes the significant fields shown in the display.

Table 127 show crypto session Field Descriptions

Field	Description
Interface	Interface to which the crypto session is related.
Session status	Current status of the crypto (VPN) sessions. See Table 128 for explanations of the status of the IKE SA, IPsec SA, and tunnel as shown in the display.
IKE SA	Information about the IKE SA, such as local and remote address and port, SA status, SA capabilities, crypto engine connection ID, and remaining lifetime of the IKE SA.
IPSEC FLOW	A snapshot of information about the IPsec-protected traffic flow, such as the status of the flow (for example, permit IP host 10.1.1.5 host 10.1.2.5), the number of IPsec SAs, the origin of the SA, such as manually entered, dynamic, or static crypto maps, number of encrypted or decrypted packets or dropped packets, and the IPsec SA remaining lifetime in kilobytes per second.

Table 128 provides an explanation of the current status of the VPN sessions shown in the display.

Table 128 Current Status of the VPN Sessions

IKE SA	IPsec SA	Tunnel Status
Exist, active	Exist (flow exists)	UP-ACTIVE
Exist, active	None (flow exists)	UP-IDLE
Exist, active	None (no flow)	UP-IDLE
Exist, inactive	Exist (flow exists)	UP-NO-IKE
Exist, inactive	None (flow exists)	DOWN-NEGOTIATING
Exist, inactive	None (no flow)	DOWN-NEGOTIATING
None	Exist (flow exists)	UP-NO-IKE
None	None (flow exists)	DOWN
None	None (no flow)	DOWN

Note IPsec flow may not exist if a dynamic crypto map is being used.

The following sample output shows all crypto sessions that are in the standby state:

```
Router# show crypto session standby

Crypto session current status

Interface: Ethernet0/0
Session status: UP-STANDBY
Peer: 10.165.200.225 port 500
  IKE SA: local 10.165.201.3/500 remote 10.165.200.225/500 Active
  IKE SA: local 10.165.201.3/500 remote 10.165.200.225/500 Active
```

```
IPSEC FLOW: permit ip host 192.168.0.1 host 172.16.0.1
      Active SAs: 4, origin: crypto map
```

Related Commands

Command	Description
clear crypto session	Deletes crypto sessions (IPsec and IKE SAs).
description	Adds a description for an IKE peer.
show crypto isakmp peer	Displays peer descriptions.

show crypto session group

To display groups that are currently active on the Virtual Private Network (VPN) device, use the **show crypto session group** command in privileged EXEC mode.

show crypto session group

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

If the **crypto isakmp client configuration group** command and **max-users** keyword have not been enabled in any VPN group profile, this command will yield a blank result.

Examples

The following example shows that at least one session is active for the group Connections:

```
Router# show crypto session group

 Group: Connections
 cisco: 1
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.
show crypto session summary	Displays groups that are currently active on the VPN device and the users that are connected for each of those groups.

show crypto session summary

To display groups that are currently active on the Virtual Private Network (VPN) device and the users that are connected for each of those groups, use the **show crypto session summary** command in privileged EXEC mode.

show crypto session summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

If the **crypto isakmp client configuration group** command and **max-users** keyword are not enabled in any VPN group profile and the **crypto isakmp client configuration group** command and **max-logins** keyword are not enabled, this command will yield a blank result.

Examples

The following example shows that the group “cisco” is active and that it has one user connected, green, who is connected one time. The number in parentheses (1) is the number of simultaneous logins for that user.

```
Router# show crypto session summary

 Group cisco has 1 connections
  User (Logins)
  green (1)
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.
show crypto session group	Displays groups that are currently active on the VPN device.

show crypto socket

To list crypto sockets, use the **show crypto socket** command in privileged EXEC mode.

show crypto socket

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.4(5)	The Flags field was added to command output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.

Usage Guidelines

Use this command to list crypto sockets and the state of the sockets.

Examples

The following sample output shows the number of crypto socket connections (2) and their state:

```
Router# show crypto socket

Number of Crypto Socket connections 2

   Tu0 Peers (local/remote): 192.168.2.2/192.168.1.1
       Local Ident  (addr/mask/port/prot): (192.168.2.2/255.255.255.255/0/47)
       Remote Ident (addr/mask/port/prot): (192.168.1.1/255.255.255.255/0/47)
       Flags: shared
       Socket State: Open
       Client: "TUNNEL SEC" (Client State: Active)
   Tu1 Peers (local/remote): 192.168.2.2/192.168.1.3
       Local Ident  (addr/mask/port/prot): (192.168.2.2/255.255.255.255/0/47)
       Remote Ident (addr/mask/port/prot): (192.168.1.3/255.255.255.255/0/47)
       Flags: shared
       Socket State: Open
       Client: "TUNNEL SEC" (Client State: Active)

Crypto Sockets in Listen state:
Client: "TUNNEL SEC" Profile: "dmvpn-profile" Map-name: "dmvpn-profile-head-2"
```

Table 129 describes the significant fields in the display.

Table 129 show crypto socket Field Descriptions

Field	Description
Number of Crypto Socket connections	Number of crypto sockets in the system.
Socket State	This state can be Open, which means that active IPSec security associations (SAs) exist, or it can be Closed, which means that no active IPSec SAs exist.
Client	Application name and its state.
Flags	If this field says “shared,” the socket is shared with more than one tunnel interface.
Crypto Sockets in Listen state	Name of the crypto IPSec profile.

show crypto tech-support

To display the crypto technical support information, use the **show crypto tech-support** command in privileged EXEC mode.

show crypto tech-support [**peer** *ip-address* | **vrf** *vrf-name*]

Syntax Description

peer	(Optional) Displays the crypto technical support information related to a peer.
ip-address	(Optional) The peer IPv4 address.
vrf	(Optional) Displays the crypto technical support information related to VPN routing or forwarding (VRF).
vrf-name	(Optional) The VRF name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

Use the optional keywords and arguments to display the specific crypto technical support information.

Examples

The following is sample output from the **show crypto tech-support** command. The fields are self-explanatory.

```
Router# show crypto tech-support

------------------ show crypto session remote 1.0.1.2 detail ------------------

------------------ show crypto ipsec sa peer 1.0.1.2 detail ------------------

------------------ show crypto isakmp sa peer 1.0.1.2 detail ------------------

IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status

------------------ show crypto isakmp peers 1.0.1.2  ------------------

------------------ show crypto ruleset detail ------------------

------------------ show processes memory | include  Crypto IKMP ----------------

 240   0       7112        252      20064           0           0 Crypto IKMP

------------------ show processes cpu |  include Crypto IKMP ------------------

 240           0         3           0  0.00%  0.00%  0.00%   0 Crypto IKMP

------------------ show crypto eli ------------------
```

```
Hardware Encryption : ACTIVE
 Number of hardware crypto engines = 1

 CryptoEngine Onboard VPN details: state = Active
 Capability      : IPPCP, DES, 3DES, AES, IPv6, FAILCLOSE

 IPSec-Session :     0 active,  1400 max, 0 failed


------------------ show cry engine accelerator statistic ------------------
Device:   Onboard VPN
Location: Onboard: 0
        :Statistics for encryption device since the last clear
         of counters 1818819 seconds ago
                      0 packets in                          0 packets out
                      0 bytes in                            0 bytes out
                      0 paks/sec in                         0 paks/sec out
                      0 Kbits/sec in                        0 Kbits/sec out
                      0 packets decrypted                   0 packets encrypte
                      0 bytes before decrypt                0 bytes encrypted
                      0 bytes decrypted                     0 bytes after encr
                      0 packets decompressed                0 packets compress
                      0 bytes before decomp                 0 bytes before com
                      0 bytes after decomp                  0 bytes after comp
                      0 packets bypass decompr              0 packets bypass cs
                      0 bytes bypass decompres              0 bytes bypass comi
                      0 packets not decompress              0 packets not compd
                      0 bytes not decompressed              0 bytes not compre
                    1.0:1 compression ratio               1.0:1 overall
                  Last 5 minutes:
                      0 packets in                          0 packets out
```

show crypto vlan

To display the VPN running state for an IPSec VPN SPA, use the **show crypto vlan** command in privileged EXEC mode.

show crypto vlan

Defaults

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)SXE2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When you show the configuration, the crypto engine subslot configuration state is expressed in the context of the associated interface VLAN. The interface VLAN is also shown as having been added to the appropriate inside trunk port. This is the case even if the configuration was loaded from a legacy (pre-crypto engine subslot) configuration file, or if VLANs were manually added instead of being added through the **crypto engine subslot** command.

Examples

In the following example, the interface VLAN belongs to the IPSec VPN SPA inside port:

```
Router# show crypto vlan
  Interface VLAN 2 on IPSec Service Module port 7/1/1 connected to Fa8/3
```

In the following example, VLAN 2 is the interface VLAN and VLAN 2022 is the hidden VLAN:

```
Router# show crypto vlan
Interface VLAN 2 on IPSec Service Module port 3/1/1 connected to VLAN 2022 with crypto map
set coral2
```

In the following example, either the interface VLAN is missing on the IPSec VPN SPA inside port, the IPSec VPN SPA is removed from the chassis, or the IPSec VPN SPA was moved to a different subslot:

```
Router# show crypto vlan
  Interface VLAN 2 connected to VLAN 3 (no IPSec Service Module attached)
```

Related Commandss

Command	Description
crypto connect vlan	Creates an interface VLAN for an IPSec VPN SPA and enters crypto-connect mode.
crypto engine subslot	Assigns an interface VLAN that requires encryption to the IPSec VPN SPA.

show diameter peer

To display the configuration and status of a specific Diameter peer, or all Diameter peers, use the **show diameter peer** command in privileged EXEC mode.

show diameter peer [*peer-name*]

Syntax Description

peer-name	Displays the configuration and status of the specified Diameter peer. **Note** If no peer name is specified, the command will display information for all configured Diameter peers.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command displays the peer status information, as well as counters, including:

- Total packets sent
- Total responses seen
- Packets with responses
- Packets without responses
- Average response delay (ms)
- Number of Diameter timeouts
- Buffer allocation failures

Examples

The following is a sample output from the **show diameter peer** command:

```
Router# show diameter peer iwan-view5

Peer information for iwan-view5
-------------------------------
Peer name: iwan-view 5
Peer type: Server
Peer transport protocol: TCP
Peer listening port: 3688
Peer security protocol: IPSEC
Peer connection timer value: 30 seconds
Peer watch dog timer value: 35 seconds
Peer vrf name: default
Peer connection status: UP
```

The fields shown above are self-explanatory.

Related Commands

Command	Description
debug diameter	Displays information about the Diameter protocol.

show dmvpn

To display Dynamic Multipoint VPN (DMVPN)-specific session information, use the **show dmvpn** command in privileged EXEC mode.

show dmvpn [**ipv4** [**vrf** *vrf-name*] | **ipv6** [**vrf** *vrf-name*]] [**debug-condition** | [**interface tunnel** *number* | **peer** {**nbma** *ip-address* | **network** *network-mask* | **tunnel** *ip-address*}] [**static**] [**detail**]]

Syntax Description

ipv4	(Optional) Displays information about IPv4 private networks.
vrf *vrf-name*	(Optional) Displays information based on the specified virtual routing and forwarding (VRF) instance.
ipv6	(Optional) Displays information about IPv6 private networks.
debug-condition	(Optional) Displays DMVPN conditional debugging.
interface	(Optional) Displays DMVPN information based on a specific interface.
tunnel	(Optional) Displays DMVPN information based on the peer Virtual Private Network (VPN) address.
number	(Optional) The tunnel address for a DMVPN peer.
peer	(Optional) Displays information for a specific DMVPN peer.
nbma	Displays DMVPN information based on nonbroadcast multiaccess (NBMA) addresses.
ip-address	The DMVPN peer IP address.
network *network-mask*	Displays DMVPN information based on a specific destination network and mask address.
static	(Optional) Displays only static DMVPN information.
detail	(Optional) Displays detail DMVPN information for each session, including Next Hop Server (NHS) and NHS status, crypto session information, and socket details.

Command Default

Information is displayed for all DMVPN-specific sessions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.4(20)T	This command was modified. The following were added: **ipv4**, **ipv6**, *ipv6-address*, **network,** and *ipv6-address*.
12.4(22)T	This command was modified. The output of this command was extended to display the NHRP group received from the spoke and the Quality of Service (QoS) policy applied to the spoke tunnel.

Usage Guidelines

Use this command to obtain DMVPN-specific session information. By default, summary information will be displayed.

When the **detail** keyword is used, command output will include information from the **show crypto session detail** command, including inbound and outbound security parameter indexes (SPIs) and the **show crypto socket** command.

Examples

The following example shows sample summary output:

```
Router# show dmvpn

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer

! The line below indicates that the sessions are being displayed for Tunnel1.
! Tunnel1 is acting as a spoke and is a peer with three other NBMA peers.

Tunnel1, Type: Spoke, NBMA Peers: 3,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     2    192.0.2.21       192.0.2.116   IKE     3w0d D
     1    192.0.2.102      192.0.2.11   NHRP 02:40:51 S
     1    192.0.2.225      192.0.2.10     UP     3w0d S

Tunnel2, Type: Spoke, NBMA Peers: 1,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1      192.0.2.25     192.0.2.171   IKE    never S
```

Table 130 describes the significant fields shown in the display.

Table 130 show dmvpn Field Descriptions

Field	Description
# Ent	The number of Next Hop Routing Protocol (NHRP) entries in the current session.
Peer NBMA Addr	The remote NBMA address.
Peer Tunnel Add	The remote tunnel endpoint IP address.
State	The state of the DMVPN session. The DMVPN session is either up or down. If the DMVPN state is down, the reason for the down state error is displayed—Internet Key Exchange (IKE), IPsec, or NHRP.
UpDn Tm	Displays how long the session has been in the current state.
Attrib	Displays any associated attributes of the current session. One of the following attributes will be displayed—dynamic (D), static (S), incomplete (I), Network Address Translation (NAT) for the peer address, or NATed, (N), local (L), no socket (X).

The following example shows output of the **show dmvpn** command with the **detail** keyword:

```
Router# show dmvpn detail

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
-------------- Interface Tunnel1 info: --------------
Intf. is up, Line Protocol is up, Addr. is 192.0.2.5
   Source addr: 192.0.2.229, Dest addr: MGRE
  Protocol/Transport: "multi-GRE/IP", Protect "gre_prof",
Tunnel VRF "" ip vrf forwarding ""
NHRP Details: NHS: 192.0.2.10 RE 192.0.2.11  E
Type: Spoke, NBMA Peers: 4
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    2        192.0.2.21      192.0.2.116    UP 00:14:59 D      192.0.2.118/24
                                            UP 00:14:59 D      192.0.2.116/32

  IKE SA: local 192.0.2.229/500 remote 192.0.2.21/500 Active
          Capabilities:(none) connid:1031 lifetime:23:45:00
  Crypto Session Status: UP-ACTIVE
  fvrf: (none)
  IPSEC FLOW: permit 47 host 192.0.2.229 host 192.0.2.21
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 1 drop 0 life (KB/Sec) 4494994/2700
        Outbound: #pkts enc'ed 1 drop 0 life (KB/Sec) 4494994/2700
   Outbound SPI : 0xD1EA3C9B, transform : esp-3des esp-sha-hmac
    Socket State: Open

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1     192.0.2.229       192.0.2.5    UP 00:15:00 DLX        192.0.2.5/32

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1     192.0.2.102      192.0.2.11 NHRP 02:55:47  S         192.0.2.11/32

  IKE SA: local 192.0.2.229/4500 remote 192.0.2.102/4500 Active
          Capabilities:N connid:1028 lifetime:11:45:37
  Crypto Session Status: UP-ACTIVE
  fvrf: (none)
  IPSEC FLOW: permit 47 host 192.0.2.229 host 192.0.2.102
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 199056 drop 393401 life (KB/Sec) 4560270/1524
        Outbound: #pkts enc'ed 416631 drop 10531 life (KB/Sec) 4560322/1524
   Outbound SPI : 0x9451AF5C, transform : esp-3des esp-sha-hmac
    Socket State: Open
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1     192.0.2.225      192.0.2.10    UP     3w0d S         192.0.2.10/32

  IKE SA: local 192.0.2.229/500 remote 192.0.2.225/500 Active
          Capabilities:(none) connid:1030 lifetime:03:46:44
  Crypto Session Status: UP-ACTIVE
  fvrf: (none)
  IPSEC FLOW: permit 47 host 192.0.2.229 host 192.0.2.225
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 430261 drop 0 life (KB/Sec) 4415197/3466
        Outbound: #pkts enc'ed 406232 drop 4 life (KB/Sec) 4415197/3466
   Outbound SPI : 0xAF3E15F2, transform : esp-3des esp-sha-hmac
    Socket State: Open

 -------------- Interface Tunnel2 info: --------------
```

```
Intf. is up, Line Protocol is up, Addr. is 192.0.2.172
   Source addr: 192.0.2.20, Dest addr: MGRE
  Protocol/Transport: "multi-GRE/IP", Protect "gre_prof",
Tunnel VRF "" ip vrf forwarding ""

NHRP Details: NHS:         192.0.2.171  E

Type: Spoke, NBMA Peers: 1
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1      192.0.2.25     192.0.2.171  IKE     never S        192.0.2.171/32

  IKE SA: local 192.0.2.20/500 remote 192.0.2.25/500 Inactive
          Capabilities:(none) connid:0 lifetime:0
  IKE SA: local 192.0.2.20/500 remote 192.0.2.25/500 Inactive
          Capabilities:(none) connid:0 lifetime:0
  Crypto Session Status: DOWN-NEGOTIATING
  fvrf: (none)
  IPSEC FLOW: permit 47 host 192.0.2.20 host 192.0.2.25
        Active SAs: 0, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
        Outbound: #pkts enc'ed 0 drop 436431 life (KB/Sec) 0/0
   Outbound SPI : 0x       0, transform :
    Socket State: Closed

Pending DMVPN Sessions:
!There are no pending DMVPN sessions.
```

The following example shows output of the **show dmvpn** command with the **detail** keyword. This example displays the NHRP group received from the spoke and the QoS policy applied to the spoke tunnel:

```
Router# show dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incompletea
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer

 -------------- Interface Tunnel0 info: --------------
Intf. is up, Line Protocol is up, Addr. is 10.0.0.1
   Source addr: 172.17.0.1, Dest addr: MGRE
  Protocol/Transport: "multi-GRE/IP", Protect "dmvpn-profile",
Tunnel VRF "", ip vrf forwarding ""

NHRP Details:
Type:Hub, NBMA Peers:2
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1      172.17.0.2        10.0.0.2    UP 00:19:57 D           10.0.0.2/32
NHRP group: test-group-0
 Output QoS service-policy applied: queueing

  IKE SA: local 172.17.0.1/500 remote 172.17.0.2/500 Active
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 172.17.0.2
  IPSEC FLOW: permit 47 host 172.17.0.1 host 172.17.0.2
        Active SAs: 2, origin: crypto map
   Outbound SPI : 0x44E4E634, transform : esp-des esp-sha-hmac
    Socket State: Open
  IKE SA: local 172.17.0.1/500 remote 172.17.0.2/500 Active
  IPSEC FLOW: permit 47 host 172.17.0.1 host 172.17.0.2
        Active SAs: 2, origin: crypto map
   Outbound SPI : 0x44E4E634, transform : esp-des esp-sha-hmac
    Socket State: Open
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
```

```
----- --------------- --------------- ----- -------- ----- -----------------
    1      172.17.0.3        10.0.0.3    UP 00:02:21 D           10.0.0.3/32
NHRP group: test-group-0
 Output QoS service-policy applied: queueing

  IKE SA: local 172.17.0.1/500 remote 172.17.0.3/500 Active
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 172.17.0.3
  IPSEC FLOW: permit 47 host 172.17.0.1 host 172.17.0.3
        Active SAs: 2, origin: crypto map
   Outbound SPI : 0xBF13C9CC, transform : esp-des esp-sha-hmac
    Socket State: Open
  IKE SA: local 172.17.0.1/500 remote 172.17.0.3/500 Active
  IPSEC FLOW: permit 47 host 172.17.0.1 host 172.17.0.3
        Active SAs: 2, origin: crypto map
   Outbound SPI : 0xBF13C9CC, transform : esp-des esp-sha-hmac
    Socket State: Open

 -------------- Interface Tunnel1 info: --------------
Intf. is up, Line Protocol is up, Addr. is 11.0.0.1
   Source addr: 172.17.0.1, Dest addr: MGRE
  Protocol/Transport: "multi-GRE/IP", Protect "dmvpn-profile",
Tunnel VRF "", ip vrf forwarding ""

NHRP Details:
Type:Hub, NBMA Peers:1
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1      172.17.0.2        11.0.0.2    UP 00:20:01 D           11.0.0.2/32
NHRP group: test-group-1
 Output QoS service-policy applied: queueing


Pending DMVPN Sessions:
```

The following example shows DMVPN debug-condition information:

```
Router# show dmvpn debug-condition

NBMA addresses under debug are:
Interfaces under debug are:
Tunnel101,
Crypto DMVPN filters:
Interface = Tunnel101
DMVPN Conditional debug context unmatched flag: OFF
```

Related Commands

Command	Description
debug dmvpn	Debugs DMVPN sessions.
show crypto session detail	Displays detailed status information for active crypto sessions.
show crypto socket	Lists crypto sockets.
show policy-map mgre	Displays statistics about a specific QoS policy as it is applied to a tunnel endpoint.

show dnsix

To display state information and the current configuration of the DNSIX audit writing module, use the **show dnsix** command in privileged EXEC mode.

show dnsix

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show dnsix** command:

```
Router# show dnsix

Audit Trail Enabled with Source 192.168.2.5
          State: PRIMARY
          Connected to 192.168.2.4
          Primary 192.168.2.4
          Transmit Count 1
          DMDP retries 4
          Authorization Redirection List:
               192.168.2.4
          Record count: 0
          Packet Count: 0
          Redirect Rcv: 0
```

show dot1x

To display details for an identity profile, use the **show dot1x** command in privileged EXEC mode.

Note Effective with Cisco IOS Release 12.2(33)SXI, the **show dot1x** command is supplemented by the **show authentication** command. The **show dot1x** command is reserved for displaying output specific to the use of the 802.1X authentication method. The **show authentication sessions** command has a wider remit of displaying information for all authentication methods and authorization features. See the **show authentication sessions** command for more information.

show dot1x [**all** [**summary**] | **interface** *interface-name*] [**details** | **statistics**]]

Syntax Description

all	(Optional) Displays 802.1X status for all interfaces.
summary	(Optional) Displays summary of 802.1X status for all interfaces.
interface *interface-name*	(Optional) Specifies the interface name and number.
details	(Optional) Displays the interface configuration as well as the authenticator instances on the interface.
statistics	(Optional) Displays 802.1X statistics for all the interfaces.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(11)AX	This command was introduced.
12.1(14)EA1	The **all** keyword was added.
12.3(2)XA	This command was integrated into Cisco IOS Release 12.3(2)XA.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)SED	The output display was expanded to include auth-fail-vlan information in the authorization state machine state and port status fields.
12.2(25)SEE	The **details** and **statistics** keywords were added.
12.3(11)T	The PAE, HeldPeriod, StartPeriod, and MaxStart fields were added to the **show dot1x** command output.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you do not specify a port, global parameters and a summary appear. If you specify a port, details for that port appear in the output.

Note In some IOS versions, the **show dot1x** command may not display the AUTHORIZED or UNAUTHORIZED value in the Port Status command output field if authentication methods other than the 802.1X authentication method are used. If the Port Status field does not contain a value, then use the **show authentication sessions** command to display the Authz Success or Authz Failed port status authentication value.

Examples

The following is sample output from the **show dot1x** command using both the **interface** and **details** keywords. The clients are successfully authenticated in this example.

```
Router# show dot1x interface ethernet1/0 details

Dot1x Info for Ethernet1/0
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 1
TxPeriod                  = 30

Dot1x Authenticator Client List
-------------------------------
Supplicant                = aabb.cc00.c901
Session ID                = 0A3462800000000000009F8
    Auth SM State         = AUTHENTICATED
    Auth BEND SM State    = IDLE
```

The following is sample output from the **show dot1x** command using both the **interface** and **details** keywords. The clients are unsuccessful at authenticating in this example.

```
Router# show dot1x interface ethernet1/0 details

Dot1x Info for Ethernet1/0
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 1
TxPeriod                  = 30

Dot1x Authenticator Client List Empty
```

Table 131 describes the significant fields shown in the displays.

Table 131 show dot1x Field Descriptions

Field	Description
PAE	Port Access Entity. Defines the role of an interface (as a supplicant, as an authenticator, or as an authenticator and supplicant).
PortControl	Port control value. • AUTO—The authentication status of the client PC is being determined by the authentication process. • Force-authorize—All the client PCs on the interface are being authorized. • Force-unauthorized—All the client PCs on the interface are being unauthorized.
ControlDirection	Indicates whether control for an IEEE 802.1X controlled port is applied to both directions (ingress and egress), or inbound direction only (ingress). See 'dot1x control-direction', or effective from Cisco IOS Release 12.2(33)SXI onwards, authentication control-direction for more detail.
HostMode	Indicates whether the host-mode is single-host or multi-host, and effective from Cisco IOS Release 12.2(33)SXI onwards, multi-auth or multi-domain as well. See 'dot1x host-mode', or effective from Cisco IOS Release 12.2(33)SXI onwards, 'authentication host-mode' for more detail.
QuietPeriod	If authentication fails for a client, the authentication gets restarted after the quiet period shown in seconds.
ServerTimeout	Timeout that has been set for RADIUS retries. If an 802.1X packet is sent to the server and the server does not send a response, the packet will be sent again after the number of seconds that are shown.
SuppTimeout	Time that has been set for supplicant (client PC) retries. If an 802.1X packet is sent to the supplicant and the supplicant does not send a response, the packet will be sent again after the number of seconds that are shown.
ReAuthMax	The maximum amount of time in seconds after which an automatic reauthentication of a client PC is initiated.
MaxReq	Maximum number of times that the router sends an Extensible Authentication Protocol (EAP) request/identity frame (assuming that no response is received) to the client PC before concluding that the client PC does not support 802.1X.
TxPeriod	Timeout for supplicant retries, that is the timeout for EAP Identity Requests. See 'dot1x timeout tx-period' for more detail.
Supplicant	MAC address of the client PC or any 802.1X client.
Session ID	The ID of the network session.

Table 131 show dot1x Field Descriptions (continued)

Field	Description
Auth SM State	Describes the state of the client PC as either AUTHENTICATED or UNAUTHENTICATED.
Auth BEND SM State	The state of the IEEE 802.1X authenticator backend state machine.

Related Commands

Command	Description
clear dot1x	Clears 802.1X interface information.
debug dot1x	Displays 802.1X debugging information.
dot1x default	Resets the global 802.1X parameters to their default values.
identity profile	Creates an identity profile.
show authentication sessions	Displays information about current Authentication Manager sessions.

show dot1x (EtherSwitch)

To display the 802.1X statistics, administrative status, and operational status for the Ethernet switch network module or for the specified interface, use the **show dot1x** command in privileged EXEC mode.

show dot1x [**statistics**] [**interface** *interface-type interface-number*]

Syntax Description

statistics	(Optional) Displays 802.1X statistics.
interface *interface-type interface-number*	(Optional) Specifies the slot and port number of the interface to reauthenticate.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

If you do not specify an interface, global parameters and a summary appear. If you specify an interface, details for that interface appear.

If you specify an interface with the **statistics** keyword, statistics appear for all physical ports.

Examples

The following is sample output from the **show dot1x** command:

```
Router# show dot1x

Global 802.1X Parameters
    reauth-enabled               no
    reauth-period              3600
    quiet-period                 60
    tx-period                    30
    supp-timeout                 30
    server-timeout               30
    reauth-max                    2
    max-req                       2

802.1X Port Summary
    Port Name               Status      Mode                Authorized
    Gi0/1                   disabled    n/a                 n/a
    Gi0/2                   enabled     Auto (negotiate)    no

    802.1X Port Details
    802.1X is disabled on GigabitEthernet0/1
```

```
802.1X is enabled on GigabitEthernet0/2
      Status                Unauthorized
      Port-control          Auto
      Supplicant            0060.b0f8.fbfb
      Multiple Hosts        Disallowed
      Current Identifier    2

      Authenticator State Machine
        State               AUTHENTICATING
        Reauth Count        1

      Backend State Machine
        State               RESPONSE
        Request Count       0
        Identifier (Server) 2

      Reauthentication State Machine
        State               INITIALIZE
```

Table 132 describes the significant fields shown in the display.

Table 132 show dot1x Field Descriptions

Field	Description
reauth-enabled	Periodic reauthentication of client PCs on the interface has been enabled or disabled.
reauth-period	Time, in seconds, after which an automatic reauthentication will be initiated.
quiet-period	After authentication fails for a client, the authentication gets restarted after this quiet period shown in seconds.
tx-period	Time, in seconds, that the device waits for a response from a client to an Extensible Authentication Protocol (EAP) request or identity frame before retransmitting the request.
supp-timeout	Time, in seconds, that has been set for supplicant (client PC) retries. If an 802.1X packet is sent to the supplicant and the supplicant does not send a response, the packet will be sent again after the number of seconds that are shown.
server-timeout	Timeout, in seconds, that has been set for RADIUS retries. If an 802.1X packet is sent to the server and the server does not send a response, the packet will be sent again after the number of seconds that are shown.
reauth-max	The maximum number of times that the device tries to authenticate the client without receiving any response before the switch resets the port and restarts the authentication process.
max-req	Maximum number of times that the router sends an EAP request/identity frame (assuming that no response is received) to the client PC before concluding that the client PC does not support 802.1X.
Port Name	Interface type and slot/port numbers.
Status	Displays the 802.1X status of the port as either enabled or disabled.

Table 132 show dot1x Field Descriptions (continued)

Field	Description
Mode	Operational status of the port: • Auto—The port control value has been configured to be Force-unauthorized but the port has not changed to that state. • n/a—802.1X is disabled.
Authorized	Authorization state of the port.
Status	Status of the port (authorized or unauthorized). The status of a port appears as authorized if the **dot1x port-control** interface configuration command is set to **auto**, and authentication was successful.
Port-control	Setting of the **dot1x port-control** interface configuration command. The port control value is one of the following: • Auto—The authentication status of the client PC is being determined by the authentication process. • Force-authorize—All the client PCs on the interface are being authorized. • Force-unauthorized—All the client PCs on the interface are being unauthorized.
Supplicant	Ethernet MAC address of the client, if one exists. If the device has not discovered the client, this field displays *Not set*.
Multiple Hosts	Setting of the **dot1x multiple-hosts** interface configuration command (allowed or disallowed).
Current Identifier	Each exchange between the device and the client includes an identifier, which matches requests with responses. This number is incremented with each exchange and can be reset by the authentication server. **Note** This field and the remaining fields in the output show internal state information. For a detailed description of these state machines and their settings, refer to the IEEE 802.1X standard.

The following is sample output from the **show dot1x interface gigabitethernet0/2** privileged EXEC command. Table 132 describes the fields in the output.

```
Router# show dot1x interface gigabitethernet0/2

802.1X is enabled on GigabitEthernet0/2
  Status                Authorized
  Port-control          Auto
  Supplicant            0060.b0f8.fbfb
  Multiple Hosts        Disallowed
  Current Identifier    3

  Authenticator State Machine
    State               AUTHENTICATED
    Reauth Count        0
```

```
  Backend State Machine
    State               IDLE
    Request Count       0
    Identifier (Server) 2

Reauthentication State Machine
    State               INITIALIZE
```

The following is sample output from the **show dot1x statistics interface gigiabitethernet0/1** command. Table 133 describes the fields in the example.

```
Router# show dot1x statistics interface gigabitethernet0/1

GigabitEthernet0/1

    Rx: EAPOL     EAPOL     EAPOL     EAPOL     EAP       EAP       EAP
        Start     Logoff    Invalid   Total     Resp/Id   Resp/Oth  LenError
        0         0         0         21        0         0         0

        Last      Last
        EAPOLVer  EAPOLSrc
        1         0002.4b29.2a03

    Tx: EAPOL     EAP       EAP
        Total     Req/Id    Req/Oth
        622       445       0
```

Table 133 show dot1x statistics Field Descriptions

Field	Description
Rx EAPOL Start	Number of valid EAPOL-start frames that have been received. **Note** EAPOL = Extensible Authentication Protocol over LAN
Rx EAPOL Logoff	Number of EAPOL-logoff frames that have been received.
Rx EAPOL Invalid	Number of EAPOL frames that have been received and have an unrecognized frame type.
Rx EAPOL Total	Number of valid EAPOL frames of any type that have been received.
Rx EAP Resp/ID	Number of EAP-response/identity frames that have been received.
Rx EAP Resp/Oth	Number of valid EAP-response frames (other than response/identity frames) that have been received.
Rx EAP LenError	Number of EAPOL frames that have been received in which the packet body length field is invalid.
Last EAPOLVer	Protocol version number carried in the most recently received EAPOL frame.
LAST EAPOLSrc	Source MAC address carried in the most recently received EAPOL frame.
Tx EAPOL Total	Number of EAPOL frames of any type that have been sent.
Tx EAP Req/Id	Number of EAP-request/identity frames that have been sent.
Tx EAP Req/Oth	Number of EAP-request frames (other than request/identity frames) that have been sent.

Related Commands

Command	Description
dot1x default	Resets the global 802.1X parameters to their default values.

show dss log

To display the invalidation routes for the DSS range on the NetFlow table in the EXEC command mode, use the **show dss log** command.

show dss log {**ip** | **ipv6**}

Syntax Description

ip	Displays the range-invalidation profile for the DSS IP.
ipv6	Displays the range-invalidation profile for the DSS IPv6.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17b)SXA	This command was changed to support the **ipv6** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

This command is not supported in Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Whenever an IPv6 entry is deleted from the routing table, a message is sent to the switch processor to remove the entries that are associated to that network. Several IPv6 prefixes are collapsed to the less specific one if too many invalidations occur in a short period of time.

Examples

This example shows how to display the range-invalidation profile for the DSS IP:

```
Router# show dss log ip

22:50:18.551  prefix 172.20.52.18 mask 172.20.52.18
22:50:20.059  prefix 127.0.0.0 mask 255.0.0.0
22:51:48.767  prefix 172.20.52.18 mask 172.20.52.18
22:51:52.651  prefix 0.0.0.0 mask 0.0.0.0
22:53:02.651  prefix 0.0.0.0 mask 0.0.0.0
22:53:19.651  prefix 0.0.0.0 mask 0.0.0.0
Router#
```

show eap registrations

To display Extensible Authentication Protocol (EAP) registration information, use the **show eap registrations** command in privileged EXEC mode.

show eap registrations [**method** | **transport**]

Syntax Description

method	(Optional) Displays information about EAP method registrations only.
transport	(Optional) Displays information about EAP transport registrations only.

Command Default

If a keyword is not used, information is displayed for all lower layers used by EAP and for the methods that are registered with the EAP framework.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)SEE	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Usage Guidelines

This command is used to check which EAP methods are enabled on a router.

Examples

The following is an example of output from the **show eap registrations** command:

```
Router# show eap registrations

Registered EAP Methods:
Method Type Name
4 Peer MD5
Registered EAP Lower Layers:
Handle Type Name
2 Authenticator Dot1x-Authenticator
1 Authenticator MAB
```

The following is an example of output from the **show eap registrations** command using the transport keyword:

```
Router# show eap registrations transport

Registered EAP Lower Layers:
Handle Type Name
2 Authenticator Dot1x-Authenticator
```

The output fields are self-explanatory.

Related Commands

Command	Description
clear eap	Clears EAP session information for the switch or specified port.

show eap sessions

To display active Extensible Authentication Protocol (EAP) session information, use the **show eap sessions** command in privileged EXEC mode.

show eap sessions [**credentials** *credentials-name* | **interface** *interface-name* | **method** *method-name* | **transport** *transport-name*]

Syntax Description

credentials *credentials-name*	(Optional) Displays information about the specified credentials profile.
interface *interface-name*	(Optional) Displays information, such as type, module, and port number, about sessions that are associated with the specified interface.
method *method-name*	(Optional) Displays information about sessions that are associated with the specified EAP method.
transport *transport-name*	(Optional) Displays information about sessions that are associated with the specified lower layer.

Command Default

All active EAP sessions are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)SEE	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Usage Guidelines

The command output can be filtered using any of the optional keywords, singly or in combination.

Examples

The following is an example of output from the **show eap sessions** command:

```
Router# show eap sessions

Role: Authenticator Decision: Fail
Lower layer: Dot1x-AuthenticaInterface: Gi1/0/1
Current method: None Method state: Uninitialised
Retransmission count: 0 (max: 2) Timer: Authenticator
ReqId Retransmit (timeout: 30s, remaining: 2s)
EAP handle: 0x5200000A Credentials profile: None
Lower layer context ID: 0x93000004 Eap profile name: None
Method context ID: 0x00000000 Peer Identity: None
Start timeout (s): 1 Retransmit timeout (s): 30 (30)
Current ID: 2 Available local methods: None
Role: Authenticator Decision: Fail
Lower layer: Dot1x-AuthenticaInterface: Gi1/0/2
Current method: None Method state: Uninitialised
Retransmission count: 0 (max: 2) Timer: Authenticator
```

```
ReqId Retransmit (timeout: 30s, remaining: 2s)
EAP handle: 0xA800000B Credentials profile: None
Lower layer context ID: 0x0D000005 Eap profile name: None
Method context ID: 0x00000000 Peer Identity: None
Start timeout (s): 1 Retransmit timeout (s): 30 (30)
Current ID: 2 Available local methods: None
.
.
.
```

The following is an example of output from the **show eap sessions interface** command:

```
Router# show eap sessions interface gigabitethernet1/0/1

Role: Authenticator Decision: Fail
Lower layer: Dot1x-AuthenticaInterface: Gi1/0/1
Current method: None Method state: Uninitialised
Retransmission count: 1 (max: 2) Timer: Authenticator
ReqId Retransmit (timeout: 30s, remaining: 13s)
EAP handle: 0x5200000A Credentials profile: None
Lower layer context ID: 0x93000004 Eap profile name: None
Method context ID: 0x00000000 Peer Identity: None
Start timeout (s): 1 Retransmit timeout (s): 30 (30)
```

The fields in the above output are self-explanatory.

Related Commands

Command	Description
clear eap sessions	Clears EAP session information for the switch or for the specified port.

show eou

To display information about Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) global values or EAPoUDP session cache entries, use the **show eou** command in privileged EXEC mode.

show eou {**all** | **authentication** {**clientless** | **eap** | **static**} | **interface** {*interface-type*} | **ip** {*ip-address*} | **mac** {*mac-address*} | **posturetoken** {*name*}} [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

all	Displays EAPoUDP information about all clients.
authentication	Authentication type.
clientless	Authentication type is clientless, that is, the endpoint system is not running Cisco Trust Agent (CTA) software.
eap	Authentication type is EAP.
static	Authentication type is statically configured.
interface	Provides information about the interface.
interface-type	Type of interface (see Table 134 for the interface types that may be shown).
ip	Specifies an IP address.
ip-address	IP address of the client device.
mac	Specifies a MAC address.
mac-address	The 48-bit address of the client device.
posturetoken	Displays information about a posture token name.
name	Name of the posture token.
begin	(Optional) Display begins with the line that matches the *expression* argument.
exclude	(Optional) Display excludes lines that match the *expression* argument.
include	(Optional) Display includes lines that match the specified *expression* argument.
expression	(Optional) Expression in the output to use as a reference point.

Command Default

All global EAPoUDP global values are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(25)SED	This command was integrated into Cisco IOS Release 12.2(25)SED.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The output of this command was enhanced to display information about whether the session is using the AAA timeout policy.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

If you do not specify a port, global parameters and a summary appear. If you specify a port, details for that port appear.

Expressions are case sensitive. For example, if you enter "**exclude output**," the lines that contain "output" are not displayed, but the lines that contain "Output" appear.

Table 134 lists the interface types that may be used for the *interface-type* argument.

Table 134 Description of Interface Types

Interface Type	Description
Async	Asynchronous interface
BVI	Bridge-Group Virtual Interface
CDMA-Ix	Code division multiple access Internet exchange (CDMA Ix) interface
CTunnel	Connectionless Network Protocol (CLNS) tunnel (Ctunnel) interface
Dialer	Dialer interface
Ethernet	IEEE 802.3 standard interface
Lex	Lex interface
Loopback	Loopback interface
MFR	Multilink Frame Relay bundle interface
Multilink	Multilink-group interface
Null	Null interface
Serial	Serial interface
Tunnel	Tunnel interface
Vif	Pragmatic General Multicast (PGM) Multicase Host interface
Virtual-PPP	Virtual PPP interface
Virtual-Template	Virtual template interface
Virtual-TokenRing	Virtual TokenRing interface

Examples

The following output displays information about a global EAPoUDP configuration. The default values can be changed or customized using the **eou default**, **eou max-retry**, **eou revalidate**, or **eou timeout** commands, depending on whether you configure them globally or on a specific interface.

```
Router# show eou

Global EAPoUDP Configuration

---------------------------
```

```
EAPoUDP Version     = 1

EAPoUDP Port        = 0x5566

Clientless Hosts    = Disabled

IP Station ID       = Disabled

Revalidation        = Enabled

Revalidation Period = 36000 Seconds

ReTransmit Period   = 3 Seconds

StatusQuery Period  = 300 Seconds

Hold Period         = 180 Seconds

AAA Timeout         = 60 Seconds

Max Retries         = 3

EAPoUDP Logging     = Disabled

Clientless Host Username = clientless

Clientless Host Password = clientless


Interface Specific EAPoUDP Configurations

----------------------------------------

Interface Ethernet2/1

  No interface specific configuration
```

The following output displays information about a global EAPoUDP configuration that includes a NAC Auth Fail Open policy for use when the AAA server is unavailable:

```
Router# show eou ip 10.0.0.1

Address : 10.0.0.1
MAC Address : 0001.027c.f364
Interface : Vlan333
AuthType : AAA DOWN
AAA Down policy : rule_policy
Audit Session ID : 00000000011C11830000000311000001
PostureToken : -------
Age(min) : 0
URL Redirect : NO URL REDIRECT
URL Redirect ACL : NO URL REDIRECT ACL
ACL Name : rule_acl
Tag Name : NO TAG NAME
User Name : UNKNOWN USER
Revalidation Period : 500 Seconds
Status Query Period : 300 Seconds
Current State : AAA DOWN
```

Table 135 describes the significant fields shown in the display

Table 135 show eou Field Descriptions

Field	Description
EAPoUDP Version	EAPoUDP protocol version.
EAPoUDP Port	EAPoUDP port number.
Clientless Hosts	Clientless hosts are enabled or disabled.
IP Station ID	Specifies whether the IP address is allowed in the AAA station-id field. By default, it is disabled.
Revalidation	Revalidation is enabled or disabled.
Revalidation Period	Specifies whether revalidation of hosts is enabled. By default, it is disabled.
ReTransmit Period	Specifies the EAPoUDP packet retransmission interval. The default is 3 seconds.
StatusQuery Period	Specifies the EAPoUDP status query interval for validated hosts. The default is 300 seconds.
Hold Period	Hold period following a failed authentication.
AAA Timeout	AAA timeout period.
Max Retries	Maximum number of allowable retransmissions.
EAPoUDP Logging	Logging is enabled or disabled.
AAA Down policy	Name of policy to be applied when the AAA server is unreachable. (This is the NAC Auth Fail Open policy.)

Related Commands

Command	Description
eou default	Sets global EAPoUDP parameters to the default values.
eou max-retry	Sets the number of maximum retry attempts for EAPoUDP.
eou rate-limit	Sets the number of simultaneous posture validations for EAPoUDP.
eou timeout	Sets the EAPoUDP timeout values.

show epm session

To display information about Enforcement Policy Module (EPM) sessions, use the **show epm session** command in privileged EXEC mode.

show epm session {**interface** *type number* | **ip** {*ip-address* [**client** *client-type*] | **all**} | **mac** {*mac-address* [**client** *client-type*] | **all**} | **summary**}

Syntax Description

interface	Displays interface based session information.
type	Interface type.
number	Interface number.
ip	Displays information specifically for an IP address.
ip-address	IP address for the session.
client	(Optional) Specifies information about the type of client.
client-type	(Optional) Type of client. Values are **cts**, **dot1x**, **eapoudp**, **mab**, and **proxy**.
mac	Displays MAC address based session information.
mac-address	MAC address of the client.
all	Displays information for all sessions.
summary	Displays summary of session information such as IP address, MAC address, and so on for all the active sessions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SXI2	This command was integrated into Cisco IOS Release 12.2(33)SXI2. The **all** keyword was added, and, **cts**, **dot1x**, and **mab** values for the *client-type* argument were added.

Examples

The following output shows information specifically for MAC address 0001.027c.f380:

```
Router# show epm session mac 0001.027c.f380 client dot1x

Admission feature       : DOT1X
AAA Policies            :
ACS ACL                 : xACSACLx-IP-VERY_SIMPLE_ACL-459b9870
SGT                     : 1357-BAD123456789
```

The following output shows information specifically for IP address 10.9.0.1:

```
Router# show epm session ip 10.9.0.1

Admission feature       : AUTHPROXY
AAA Policies            :
Input Service Policy    : epm-pol-map
Proxy ACL               : permit udp any any
```

```
Proxy ACL               : deny icmp any any
ACS ACL                 : xACSACLx-IP-VERY_SIMPLE_ACL-472594af

Admission feature       : EAPOUDP
AAA Policies            :
ACS ACL                 : xACSACLx-IP-VERY_SIMPLE_ACL-459b9870
Proxy ACL               : permit udp any any
Proxy ACL               : permit icmp any any
Proxy ACL               : permit tcp an

Admission feature       : DOT1X
AAA Policies            :
ACS ACL                 : xACSACLx-IP-VERY_SIMPLE_ACL-459b9870
SGT                     : 1357-BAD123456789
```

The following example shows summary information for all sessions:

```
Router# show epm session summary

EPM Session Information
-------------------------
Total sessions seen so far : 5
Total active sessions      : 5

Interface              IP Address          MAC Address       Audit Session Id:
-------------------------------------------------------------------------------
GigabitEthernet7/2     209.165.200.225     0001.027c.f380    160000020000000000003A4EC
GigabitEthernet7/2     209.165.200.227     0001.027c.f380    160000020000000010003AD68
GigabitEthernet7/2     209.165.200.230     0001.027c.f380    160000020000000020003C110
GigabitEthernet7/2     209.165.200.235     0001.027c.f380    160000020000000030003D6BC
GigabitEthernet7/15    0.0.0.0             0030.6eb6.c69a    0904010C000000000002F6A4
```

Table 136 describes significant fields shown in the displays.

Table 136 show epm session ip Field Descriptions

Field	Description
Admission feature	Admission feature authentication proxy or Extensible Authentication Protocol over UDP (EOU) acting on the host.
AAA Policies	AAA policy information.
ACS ACL	Access control server (ACS) access control list (ACL).
SGT	Security group tag (SGT) value assigned to the host of that initiated the session.
Input Service Policy	Input service policy for the session.
Proxy ACL	Proxy access control list.
Total sessions seen so far	Total number of hosts connected to the Network Access Device (NAD) until now.
Total active sessions	Total number of active sessions.
Interface	Interface type and number.
IP Address	IP address of the host.
MAC Address	MAC address of the host.
Audit Session Id	Audit session ID.

show firewall vlan-group

To display secure virtual LANs (VLANs) attached to a secure group, use the **show firewall vlan-group** command in user EXEC or privileged EXEC mode.

show firewall vlan-group [*number*]

Syntax Description

number	(Optional) VLAN group number. The range is from 1 to 65535.

Command Default

This command has no default settings.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI1	This command was introduced.
12.2(33)SXJ	This command was modified. The command output was modified to display the VLAN groups created by both the Application Control Engine (ACE) and firewall.

Examples

The following is sample output from the **show firewall vlan-group** command:

```
Router# show firewall vlan-group

Display vlan-groups created by both ACE module and Firewall

Group    Created by      vlans
-----    ----------      -----
  142      Firewall      142
  200      Firewall      200-201
  360      Firewall      360-369
  380      Firewall      380-389
  500      Firewall      390-399
  660      Firewall      660-669
```

Table 137 describes the fields shown in the display.

Table 137 show firewall vlan-group Field Descriptions

Field	Description
Group	Group number to which the VLANs belong.
Created by	Indicates whether the VLAN groups are created by the ACE or the firewall.
vlans	VLAN ranges.

Related Commands

Command	Description
firewall	Specifies secure VLAN groups and attaches them to firewall modules.

show fm private-hosts

To display information about the Private Hosts feature manager, use the **show fm private-hosts** command in privileged EXEC mode.

show fm private-hosts {**all** | **interface** *type*/*num*}

Syntax Description

all	Displays the feature manager information for all of the interfaces that are configured for Private Hosts.
interface *type*/*num*	Displays the feature manager information for a specific interface. The slash (/) is required.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following example displays information about the Private Hosts feature manager:

```
Router# show fm private-hosts interface GigabitEthernet1/2

------------------------------------------------------------------------------
FM_FEATURE_PVT_HOST_INGRESS      i/f: Gi1/2      map name:
PVT_HOST_ISOLATED
==============================================================================

------------------------------------------------------------
MAC Seq. No: 10          Seq. Result : PVT_HOSTS_ACTION_DENY
------------------------------------------------------------
Indx - VMR index      T     - V(Value)M(Mask)R(Result)
EtTy - Ethernet Type  EtCo  - Ethernet Code
+----+-+--------------+--------------+----+----+
|Indx|T|   Dest Node  |  Source Node |EtTy|EtCo|
+----+-+--------------+--------------+----+----+

 1    V 0000.0000.0000 0000.1111.4001    0 0
      M 0000.0000.0000 ffff.ffff.ffff    0 0
      TM_PERMIT_RESULT

 2    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_L3_DENY_RESULT

------------------------------------------------------------
MAC Seq. No: 20          Seq. Result : PVT_HOSTS_ACTION_PERMIT
------------------------------------------------------------
+----+-+--------------+--------------+----+----+
|Indx|T|   Dest Node  |  Source Node |EtTy|EtCo|
+----+-+--------------+--------------+----+----+

 1    V 0000.1111.4001 0000.0000.0000    0 0
```

```
      M ffff.ffff.ffff 0000.0000.0000    0 0
      TM_PERMIT_RESULT

 2    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_L3_DENY_RESULT

------------------------------------------------------------
MAC Seq. No: 30          Seq. Result : PVT_HOSTS_ACTION_REDIRECT
------------------------------------------------------------
+----+-+--------------+--------------+----+----+
|Indx|T|   Dest Node  |  Source Node |EtTy|EtCo|
+----+-+--------------+--------------+----+----+

 1    V ffff.ffff.ffff 0000.0000.0000    0 0
      M ffff.ffff.ffff 0000.0000.0000    0 0
      TM_PERMIT_RESULT

 2    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_L3_DENY_RESULT

------------------------------------------------------------
MAC Seq. No: 40          Seq. Result : PVT_HOSTS_ACTION_PERMIT
------------------------------------------------------------
+----+-+--------------+--------------+----+----+
|Indx|T|   Dest Node  |  Source Node |EtTy|EtCo|
+----+-+--------------+--------------+----+----+

 1    V 0100.5e00.0000 0000.0000.0000    0 0
      M ffff.ff80.0000 0000.0000.0000    0 0
      TM_PERMIT_RESULT

 2    V 3333.0000.0000 0000.0000.0000    0 0
      M ffff.0000.0000 0000.0000.0000    0 0
      TM_PERMIT_RESULT

 3    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_L3_DENY_RESULT

------------------------------------------------------------
MAC Seq. No: 50          Seq. Result : PVT_HOSTS_ACTION_DENY
------------------------------------------------------------
+----+-+--------------+--------------+----+----+
|Indx|T|   Dest Node  |  Source Node |EtTy|EtCo|
+----+-+--------------+--------------+----+----+

 1    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_PERMIT_RESULT

 2    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_L3_DENY_RESULT


Interfaces using this pvt host feature in ingress dir.:
-------------------------------------------------
  Interfaces (I/E = Ingress/Egress)
```

Related Commands

Command	Description
private-hosts	Enables or configures the private host feature.
private-hosts mode	Sets the switchport mode.
show fm private-hosts	Displays the FM-related private hosts information.
show private-hosts configuration	Displays Private Hosts configuration information for the router.
show private-hosts interface configuration	Displays Private Hosts configuration information for individual interfaces.

show fpm package-group

To display configuration information about flexible packat matching (fpm) package support, use the **show fpm package-group** command in user EXEC or privileged EXEC mode.

show fpm package-group [**control-plane** | *fpm-package-group* | **interface** *interface-name*]

Syntax Description

control-plane	(Optional) Displays fpm package group control plane information.
fpm-group-name	(Optional) Displays fpm group name information.
interface	(Optional) Displays fpm package group interface information.
interface-name	Name of the Interface for which you want to show the fpm package group information. See Table 145 for a list of valid interfaces.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Table 145 displays valid interfaces that may be shown as the *interface-name* argument with the **interface** keyword.

Table 138 Interfaces That Can Be Shown

Interface	Description
ATM	ATM interface
Async	Asynchronous interface
Auto-template	Auto-Template interface
BVI	Bridge-Group Virtual Interface
CDMA-Ix	CDMA Ix interface
CTunnel	CTunnel interface
Dialer	Dialer interface
FastEthernet	FastEthernet IEEE 802.3
Lex	Lex interface
LongReachEthernet	Long-Reach Ethernet interface
Loopback	Loopback interface
MFR	Multilink Frame Relay bundle intrface
Multilink	Multilink-group interface
Null	Null interface

Table 138 Interfaces That Can Be Shown

Interface	Description
Pos	Packet over sonet interface
Port-channel	Ethernet channel of interfaces
SSLVPN-VIF	Secure Socket Layer Virtual Private Network (SSLVPN) Virtual Interface
Serial	Serial
Tunnel	Tunnel interface
vif	Pragmatic General Multicast (PGM) multicast host interface
virtual-PPP	Virtual PPP interface
virtual-Template	Virtual template interface
virtual-TokenRing	Virtual TokenRing
vmi	Virtual Multipoint Interface

Examples

The following is sample output from the **show fpm package-group** command.

```
Router# show fpm package-group

Router# show fpm package-group
 group name: cisco-fpm-packages
  auto-load
  fpm package: fpm-package-11
  fpm package: fpm-package-43
   package action: log
```

Table 139 describes the significant fields shown in the display.

Table 139 show fpm package-group Field Descriptions

Field	Description
Auto-load	Displays if automatic loading of fpm package support is configured.
FPM package	Displays the name of the fpm package loaded from the fpm-server.
Group name	Displays the protocol to connect to the fpm-server.
Package action	Displays the action taken when the fpm package is loaded.

Related Commands

Command	Description
show fpm package-info	Displays fpm package transfer configuration details.

show fpm package-info

To display information about fpm package transfer between an fpm-server and a local server, use the **show fpm package-info** command in user EXEC or privileged EXEC mode.

show fpm package-info

Syntax Description

This command has no keywords or arguments.

Command Default

The command displays information about the transfer of fpm package groups from the fpm-server to a local server.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Examples

The following is sample output from the **show fpm package-info** command.

```
Router# show fpm package-info

Router# show fpm package-info
 fpm package-info
  host 10.0.0.1
  remote-path bluebell/
  local-path flash:
  user cisco
  password 7 0101130A5D04141D245F5A1B0C0B57
  protocol tftp
  time-range weekly
```

Table 139 describes the significant fields shown in the display.

Table 140 show fpm package-info Field Descriptions

Field	Description
Host	Displays the download server address.
Local-path	Displays the location where packages are stored on the local router.
Password	Displays and encrypted password for the server.
Protocol	Displays the protocol to connect to the server.
Remote-path	Displays the file server name.
Time-range	Displays the interval between searches for fpm updates.
User	Displays the username on the server.

Related Commands

Command	Description
show fpm package-group	Displays fpm package matching support configuration details.

show idmgr

To display information related to the Intelligent Services Gateway (ISG) session identity, use the **show idmgr** command in privileged EXEC mode.

show idmgr {**memory** [**detailed** [**component** [*substring*]]] | **service key session-handle** *session-handle-string* **service-key** *key-value* | **session key** {**aaa-unique-id** *aaa-unique-id-string* | **domainip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **nativeip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **portbundle ip** *ip-address* **bundle** *bundle-number* | **session-guid** *session-guid* | **session-handle** *session-handle-string* | **session-id** *session-id-string* | **circuit-id** *circuit-id*} | **statistics**}

Syntax Description

memory	Displays memory-usage information related to ID management.
detailed	(Optional) Displays detailed memory-usage information related to ID management.
component	(Optional) Displays information for the specified ID management component.
substring	(Optional) Substring to match the component name.
service key	Displays ID information for a specific service.
session-handle *session-handle-string*	Displays the unique identifier for a session.
service-key *key-value*	Displays ID information for a specific service.
session key	Displays ID information for a specific session and its related services.
aaa-unique-id *aaa-unique-id-string*	Displays the authentication, authorization, and accounting (AAA) unique ID for a specific session.
domainip-vrf ip-address *ip-address*	Displays the service-facing IP address for a specific session.
vrf-id *vrf-id*	Displays the VPN routing and forwarding (VRF) ID for the specific session.
nativeip-vrf ip-address *ip-address*	Displays the subscriber-facing IP address for a specific session.
portbundle ip *ip-address*	Displays the port bundle IP address for a specific session.
bundle *bundle-number*	Displays the bundle number for a specific session.
session-guid *session-guid*	Displays the global unique identifier for a session.
session-handle *session-handle-string*	Displays the session identifier for a specific session.
session-id *session-id-string*	Displays the session identifier used to construct the value for RADIUS attribute 44 (Acct-Session-ID).
circuit-id *circuit-id*	Displays the user session information in the ID Manager (IDMGR) database by specifying the unique circuit ID tag.
statistics	Displays statistics related to storing and retrieving ID information.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
Cisco IOS XE Release 2.6	The **circuit-id** keyword and *circuit-id* argument was added.

Examples The following sample output for the **show idmgr** command displays information about the service called "service":

```
Router# show idmgr service key session-handle 48000002 service-key service

session-handle = 48000002
service-name = service
idmgr-svc-key = 4800000273657276696365
authen-status = authen
```

The following sample output for the **show idmgr** command displays information about a session and the service that is related to the session:

```
Router# show idmgr session key session-handle 48000002

session-handle = 48000002
aaa-unique-id = 00000002
authen-status = authen
username = user1

Service 1 information:
session-handle = 48000002
service-name = service
idmgr-svc-key = 4800000273657276696365
```

The following sample output for the **show idmgr** command displays information about the global unique identifier of a session:

```
Router# show idmgr session key session-guid 020202010000000C

session-handle = 18000003
aaa-unique-id = 0000000C
authen-status = authen
interface = nas-port:0.0.0.0:2/0/0/42
authen-status = authen
username = FortyTwo
addr = 100.42.1.1
session-guid = 020202010000000C
```

The following sample output for the **show idmgr** command displays information about the user session information in the ID Manager (IDMGR) database by specifying the unique circuit ID tag:

```
Router# show idmgr session key circuit-id Ethernet4/0.100:PPPoE-Tag-1

session-handle = AA000007
aaa-unique-id = 0000000E
circuit-id-tag = Ethernet4/0.100:PPPoE-Tag-1
interface = nas-port:0.0.0.0:0/1/1/100
authen-status = authen
username = user1@cisco.com
addr = 106.1.1.3
session-guid = 650101020000000E
The session hdl AA000007 in the record is valid
The session hdl AA000007 in the record is valid
No service record found
```

Table 141 describes the significant fields shown in the display.

Table 141 show idmgr Field Descriptions

Field	Description
session-handle	Unique identifier of the session.
service-name	Service name for this session.
idmgr-svc-key	The ID manager service key of this session.
authen-status	Indicates whether the session has been authenticated or unauthenticated.
aaa-unique-id	AAA unique ID of the session.
username	The username associated with this session.
interface	The interface details of this session.
addr	The IP address of this session.
session-guid	Global unique identifier of this session.

Related Commands

Command	Description
subscriber access pppoe unique-key circuit-id	Specifies a unique circuit ID tag for a PPPoE user session to be tapped on the router.

show interface virtual-access

To display virtual access interface information, use the **show interface virtual-access** command in user EXEC or privileged EXEC mode.

show interface virtual-access *interface-number* [**accounting | configuration | counters protocol status | crb | dampening | description | fair-queue | irb | mpls-exp | precedence | random-detect | rate-limit | stats | summary | switching**]

Syntax Description

interface-number	Virtual access interface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
accounting	(Optional) Displays virtual access interface accounting information.
configuration	(Optional) Displays virtual access interface configuration information.
counters protocol status	(Optional) Displays information about the current status of protocol counters that are enabled.
crb	(Optional) Displays virtual access interface concurrent routing and bridging (CRB) information.
dampening	(Optional) Displays virtual access interface dampening information.
description	(Optional) Displays virtual access interface description.
fair-queue	(Optional) Displays virtual access interface weighted fair queueing (WFQ) information.
irb	(Optional) Displays virtual access interface integrated routing and bridging (IRB) information.
mpls-exp	(Optional) Displays virtual interface Multiprotocol Label Switching (MPLS) experimental accounting information.
precedence	(Optional) Displays virtual interface precedence accounting information.
random-detect	(Optional) Displays virtual interface Weighted Random Early Detection (WRED) information.
rate-limit	(Optional) Displays virtual interface rate-limit information.
stats	(Optional) Displays virtual interface packets and octets, in and out, by switching path.
summary	(Optional) Displays the virtual interface summary.
switching	(Optional) Displays virtual interface switching information.

Command Default

If no keyword is specified, general information about virtual access interfaces is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced in a release earlier than Cisco IOS Release 15.1(1)T.

Examples

The following is sample output from the **show interface virtual-access** command:

```
Router# show interface virtual-access 1

Virtual-Access1 is up, line protocol is up
Hardware is Virtual Access interface
Description: ***Internally created by SSLVPN context c3***
Interface is unnumbered. Using address of Virtual-Access1 (0.0.0.0)
MTU 1406 bytes, BW 100000 Kbit/sec, DLY 100000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation SSL
SSL vaccess, cloned from Virtual-Template1
Vaccess status 0x4, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output never, output hang never
Last clearing of "show interface" counters 2d16h
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 24 bits/sec, 10 packets/sec
5 minute output rate 16 bits/sec, 10 packets/sec
100 packets input, 2000 bytes, 23 no buffer
Received 79 broadcasts, 30 runts, 20 giants, 29 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
12 packets output, 1100 bytes, 10 underruns
6 output errors, 5 collisions, 1 interface resets
9 unknown protocol drops
10 unknown protocol drops
29 output buffer failures, 10 output buffers swapped out
25 carrier transitions
```

Table 142 describes the significant fields shown in the display.

Table 142 show interface virtual-access Field Descriptions

Field	Description
Using address of Virtual-Access1	IP address of the virtual interface.
MTU	MTU, in bytes. Default: 1500.
BW	Bandwidth, in Kb/s.
DLY	Delay, in microseconds.
reliability	Reliability of the interface as a fraction of 255. Default: Calculated as an exponential average over five minutes. • 255/255 provides 100 percent reliability.
txload	Transmission load on an interface as a fraction of 255.
rxload	Receiver load on an interface as a fraction of 255.
Encapsulation	Data-link encapsulation.
SSL vaccess	Specifies Secure Socket Layer Virtual Private Network (SSL VPN) virtual access.

Table 142 show interface virtual-access Field Descriptions (continued)

Field	Description
Vaccess status	Status of the virtual access.
ARP type	Type of Address Resolution Protocol (ARP).
ARP Timeout	Amount of time an entry remains in the ARP cache.
Input queue	Number of packets in the input queue.
Total output drops	Total number of packets dropped.
Queueing strategy	Theory followed to treat the packets in a queue.
Output queue	Number of packets in the output queue.
broadcasts	Total number of broadcast or multicast packets received.
runts	Total number of packets discarded due to the packet size being less than the minimum packet size (64 bytes).
giants	Total number of packets discarded due to the packet size exceeding the maximum packet size.
throttles	Total number of throttles.
input errors	Total number of errors that prevented the receipt of datagrams.
CRC	Mismatch generated by the cyclic redundancy checksum (CRC).
frame	Total number of packets received with a CRC error.
overrun	Total number of times data has not reached the serial receiver buffer because of the input rate is more than the receiver can handle.
ignored	Total number of packets ignored by the interface because of the scarcity of internal buffers.
abort	Total number of packets aborted.
output errors	Total number of errors that prevented the final transmission.
collisions	Total number of collisions encountered.
interface resets	Total number of times an interface has been completely reset.
output buffer failures	Total number of buffer failures.
carrier transitions	Interface transitions.

Related Commands

Command	Description
clear interface virtual-access	Clears the virtual access interface and frees the memory for other dial-in uses.

show ip access-lists

To display the contents of all current IP access lists, use the **show ip access-lists** command in user EXEC or privileged EXEC modes.

show ip access-lists [*access-list-number* | *access-list-number-expanded-range* | *access-list-name* | **dynamic** [*dynamic-access-list-name*] | **interface** *name number* [**in** | **out**]]

Syntax Description

access-list-number	(Optional) Number of the IP access list to display.
access-list-number-expanded-range	(Optional) Expanded range of the IP access list to display.
access-list-name	(Optional) Name of the IP access list to display.
dynamic *dynamic-access-list-name*	(Optional) Displays the specified dynamic IP access lists.
interface *name number*	(Optional) Displays the access list for the specified interface.
in	(Optional) Displays input interface statistics.
out	(Optional) Displays output interface statistics.

Defaults

All standard and expanded IP access lists are displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.3	This command was introduced.
12.3(7)T	The **dynamic** keyword was added.
12.4(6)T	The **interface** *name* and *number* keyword and argument pair was added. The **in** and **out** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was modified. Example output from the **dynamic** keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. The output of this command was extended to display access lists that contain object groups.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

The **show ip access-lists** command provides output identical to the **show access-lists** command, except that it is IP-specific and allows you to specify a particular access list.

Examples

The following is sample output from the **show ip access-lists** command when all access lists are requested:

```
Router# show ip access-lists

Extended IP access list 101
   deny udp any any eq nntp
   permit tcp any any
   permit udp any any eq tftp
   permit icmp any any
   permit udp any any eq domain
```

Table 143 describes the significant fields shown in the display.

Table 143 show ip access-lists Field Descriptions

Field	Description
Extended IP access list	Extended IP access-list number.
deny	Packets to reject.
udp	User Datagram Protocol.
any	Source host or destination host.
eq	Packets on a given port number.
nntp	Network News Transport Protocol.
permit	Packets to forward.
tcp	Transmission Control Protocol.
tftp	Trivial File Transfer Protocol.
icmp	Internet Control Message Protocol.
domain	Domain name service.

The following is sample output from the **show ip access-lists** command when the name of a specific access list is requested:

```
Router# show ip access-lists Internetfilter

Extended IP access list Internetfilter
   permit tcp any 192.0.2.0 255.255.255.255 eq telnet
   deny tcp any any
   deny udp any 192.0.2.0 255.255.255.255 lt 1024
   deny ip any any log
```

The following is sample output from the **show ip access-lists** command when the name of a specific access list that contains an object group is requested:

```
Router# show ip access-lists my-ogacl-policy

Extended IP access list my-ogacl-policy
   10 permit object-group eng-service any any
```

The following sample output from the **show ip access-lists** command shows input statistics for Fast Ethernet interface 0/0:

```
Router# show ip access-lists interface FastEthernet0/0 in

Extended IP access list 150 in
```

```
   10 permit ip host 10.1.1.1 any
   30 permit ip host 10.2.2.2 any (15 matches)
```

The following is sample output from the **show ip access-lists** command using the **dynamic** keyword:

```
Router# show ip access-lists dynamic CM_SF#1

Extended IP access list CM_SF#1
    10 permit udp any any eq 5060 (650 matches)
    20 permit tcp any any eq 5060
    30 permit udp any any dscp ef (806184 matches)
```

To check your configuration, use the **show run interfaces cable** command:

```
Router# show run interfaces cable 0/1/0

Building configuration...

Current configuration : 144 bytes
!
interface cable-modem0/1/0
 ip address dhcp
 load-interval 30
 no keepalive
  service-flow primary upstream
   service-policy output llq
end
```

Related Commands

Command	Description
deny	Sets conditions in a named IP access list or OGACL that will deny packets.
ip access-group	Applies an ACL or OGACL to an interface or a service policy map.
ip access-list	Defines an IP access list or OGACL by name or number.
object-group network	Defines network object groups for use in OGACLs.
object-group service	Defines service object groups for use in OGACLs.
permit	Sets conditions in a named IP access list or OGACL that will permit packets.
show object-group	Displays information about object groups that are configured.
show run interfaces cable	Displays statistics on the cable modem.

show ip admission

To display the network admission (NAC) control cache entries or the running network admission control configuration, use the **show ip admission** command in privileged EXEC mode.

show ip admission {[**cache** [**consent**]] [**configuration**] [**eapoudp**]}

Syntax Description

cache	Displays the current list of network admission entries.
consent	Displays the authentication proxy consent webpage sessions.
configuration	Displays the running network admission control configuration.
eapoudp	Displays the Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) network admission control entries.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(11)T	The output of this command was enhanced to display whether the AAA timeout policy is configured.
12.4(15)T	The **consent** keyword was added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use **show ip admission cache eapoudp** to list the host IP addresses, the session timeout, and the posture state. If the posture statue is POSTURE ESTAB, the host validation was successful.

Examples

The following output displays all the IP admission control rules that are configured on the router:

```
Router# show ip admission configuration

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication Proxy Watch-list is disabled

Authentication Proxy Rule Configuration
 Auth-proxy name avrule
    eapoudp list not specified auth-cache-time 60 minutes
```

The following output displays the host IP addresses, the session timeout, and the posture states:

```
Router# show ip admission cache eapoudp

Posture Validation Proxy Cache
Total Sessions: 3 Init Sessions: 1
 Client IP 10.0.0.112, timeout 60, posture state POSTURE ESTAB
 Client IP 10.0.0.142, timeout 60, posture state POSTURE INIT
 Client IP 10.0.0.205, timeout 60, posture state POSTURE ESTAB
```

The following output displays a configuration that includes both a global and a rule-specific NAC Auth Fail Open policy:

```
Router# show ip admission configuration

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is enabled
Watch-list expiry timeout is 1 minutes
! The line below shows the global policy:
Authentication global AAA fail identity policy aaa_fail_policy
Authentication Proxy Rule Configuration Auth-proxy name greentree
    eapoudp list 101 specified auth-cache-time 60 minutes
! The line below shows the rule-specific AAA fail policy; the name changes based on what
the user configured.
    Identity policy name aaa_fail_policy for AAA fail policy
```

The field descriptions in the display are self-explanatory.

In the following example, a session has been initiated via https://192.168.104.136 from the client 192.168.100.132. After a successful session establishment, the output is as follows:

```
Router# show ip admission cache

Authentication Proxy Cache
 Client Name N/A, Client IP 192.168.100.132, Port 1204, timeout 204, Time Remaining 204,
 state ESTAB

Router# show ip admission cache consent

Authentication Proxy Consent Cache
 Client Name N/A, Client IP 192.168.100.132, Port 1204, timeout 204, Time Remaining 204,
 state ESTAB

Router# show ip admission cache eapoudp

Posture Validation Proxy Cache
Total Sessions: 0 Init Sessions: 0
```

Related Commands

Command	Description
clear ip admission cache	Clears IP admission cache entries from the router.
ip admission name	Creates a Layer 3 network admission control rule.

show ip audit configuration

To display additional configuration information, including default values that may not be displayed using the **show running-config** command, use the **show ip audit configuration** command in EXEC mode.

show ip audit configuration

Syntax Description

This command has no argument or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show ip audit configuration** EXEC command to display additional configuration information, including default values that may not be displayed using the **show running-config** command.

Examples

The following example displays the output of the **show ip audit configuration** command:

```
Event notification through syslog is enabled
Event notification through Net Director is enabled
Default action(s) for info signatures is alarm
Default action(s) for attack signatures is alarm
Default threshold of recipients for spam signature is 25
PostOffice:HostID:5 OrgID:100 Addr:10.2.7.3 Msg dropped:0
HID:1000 OID:100 S:218 A:3 H:14092 HA:7118 DA:0 R:0
    CID:1 IP:172.21.160.20 P:45000 S:ESTAB (Curr Conn)

Audit Rule Configuration
 Audit name AUDIT.1
    info actions alarm
```

Related Commands

Command	Description
clear ip audit statistics	Resets statistics on packets analyzed and alarms sent.

show ip audit interface

To display the interface configuration, use the **show ip audit interface** command in EXEC mode.

show ip audit interface

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show ip audit interface** EXEC command to display the interface configuration.

Examples

The following example displays the output of the **show ip audit interface** command:

```
Interface Configuration
 Interface Ethernet0
  Inbound IDS audit rule is AUDIT.1
    info actions alarm
  Outgoing IDS audit rule is not set
 Interface Ethernet1
  Inbound IDS audit rule is AUDIT.1
    info actions alarm
  Outgoing IDS audit rule is AUDIT.1
    info actions alarm
```

show ip audit statistics

To display the number of packets audited and the number of alarms sent, among other information, use the **show ip audit statistics** command in EXEC mode.

show ip audit statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show ip audit statistics** EXEC command to display the number of packets audited and the number of alarms sent, among other information.

Examples

The following displays the output of the **show ip audit statistics** command:

```
Signature audit statistics [process switch:fast switch]
  signature 2000 packets audited: [0:2]
  signature 2001 packets audited: [9:9]
  signature 2004 packets audited: [0:2]
  signature 3151 packets audited: [0:12]
Interfaces configured for audit 2
Session creations since subsystem startup or last reset 11
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [2:1:0]
Last session created 19:18:27
Last statistic reset never

HID:1000 OID:100 S:218 A:3 H:14085 HA:7114 DA:0 R:0
```

Related Commands

Command	Description
clear ip audit statistics	Resets statistics on packets analyzed and alarms sent.

show ip auth-proxy

To display the authentication proxy entries or the running authentication proxy configuration, use the **show ip auth-proxy** command in privileged EXEC mode.

show ip auth-proxy {**cache** | **configuration**}

Syntax Description

cache	Displays the current list of the authentication proxy entries.
configuration	Displays the running authentication proxy configuration.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show ip auth-proxy** to display either the authentication proxy entries or the running authentication proxy configuration. Use the **cache** keyword to list the host IP address, the source port number, the timeout value for the authentication proxy, and the state for connections using authentication proxy. If authentication proxy state is HTTP_ESTAB, the user authentication was successful.

Use the **configuration** keyword to display all authentication proxy rules configured on the router.

Examples

The following example shows sample output from the **show ip auth-proxy cache** command after one user authentication using the authentication proxy:

```
Router# show ip auth-proxy cache

Authentication Proxy Cache
    Client IP 192.168.25.215 Port 57882, timeout 1, state HTTP_ESTAB
```

The following example shows how the **show ip auth-proxy configuration** command displays the information about the authentication proxy rule **pxy**. The global idle timeout value is 60 minutes. The idle timeouts value for this named rule is 30 minutes. No host list is specified in the rule, meaning that all connection initiating HTTP traffic at the interface is subject to the authentication proxy rule.

```
Router# show ip auth-proxy configuration

Authentication cache time is 60 minutes
Authentication Proxy Rule Configuration
Auth-proxy name pxy
http list not specified auth-cache-time 30 minutes
```

Related Commands

Command	Description
clear ip auth-proxy cache	Clears authentication proxy entries from the router.
ip auth-proxy	Sets the authentication proxy idle timeout value (the length of time an authentication cache entry, along with its associated dynamic user ACL, is managed after a period of inactivity).
ip auth-proxy (interface configuration)	Applies an authentication proxy rule at a firewall interface.
ip auth-proxy name	Creates an authentication proxy rule.

show ip auth-proxy watch-list

To display the information about the authentication proxy watch list in the EXEC command mode, use the **show ip auth-proxy watch-list** command.

show ip auth-proxy watch-list

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

Examples

This example shows how to display the information about the authentication proxy watch list:

```
Router# show ip auth-proxy watch-list

Authentication Proxy Watch-list is enabled
Watch-list expiry timeout is 2 minutes
Total number of watch-list entries: 3

 Source IP       Type         Violation-count
 10.0.0.2        MAX_RETRY    MAX_LIMIT
 10.0.0.3        TCP_NO_DATA  MAX_LIMIT
 10.255.255.255 CFGED        N/A

Total number of watch-listed users: 3
Router#
```

Related Commands

Command	Description
clear ip auth-proxy watch-list	Deletes a single watch-list entry or all watch-list entries.
ip auth-proxy max-login-attempts	Limits the number of login attempts at a firewall interface.
ip auth-proxy watch-list	Enables and configures an authentication proxy watch list.

show ip bgp labels

To display information about Multiprotocol Label Switching (MPLS) labels from the external Border Gateway Protocol (eBGP) route table, use the **show ip bgp labels** command in privileged EXEC mode.

show ip bgp labels

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use this command to display eBGP labels associated with an Autonomous System Boundary Router (ASBR).

This command displays labels for BGP routes in the default table only. To display labels in the Virtual Private Network (VPN) routing and forwarding (VRF) tables, use the **show ip bgp vpnv4** {**all** | **vrf** *vrf-name*} command with the optional **labels** keyword.

Examples

The following example shows output for an ASBR using BGP as a label distribution protocol:

```
Router# show ip bgp labels

Network          Next Hop         In Label/Out Label
10.3.0.0/16       0.0.0.0          imp-null/exp-null
10.15.15.15/32   10.15.15.15      18/exp-null
10.16.16.16/32   0.0.0.0          imp-null/exp-null
10.17.17.17/32   10.0.0.1         20/exp-null
10.18.18.18/32   10.0.0.1         24/31
10.18.18.18/32   10.0.0.1         24/33
```

Table 144 describes the significant fields shown in the display.

Table 144 show ip bgp labels Field Descriptions

Field	Description
Network	Displays the network address from the eGBP table.
Next Hop	Specifies the eBGP next hop address.
In Label	Displays the label (if any) assigned by this router.
Out Label	Displays the label assigned by the BGP next hop router.

Related Commands

Command	Description
show ip bgp vpnv4	Displays VPN address information from the BGP table.

show ip device tracking

To display information about entries in the IP device tracking table, use the **show ip device tracking** command in privileged EXEC mode.

show ip device tracking {**all count** | **interface** *type-of-interface* | **ip** *ip-address* | **mac** *mac-address*}

Syntax Description

all count	Displays a count of all IP tracking host entries.
interface *type-of-interface*	Displays interface information. See Table 145 for a list of valid interfaces.
ip *ip-address*	Displays the IP address of the client.
mac *mac-address*	Displays the 48-bit hardware MAC address.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2SX	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

Table 145 displays valid interfaces that may be shown as the *type-of-interface* argument with the **interface** keyword.

Table 145 Interfaces That Can Be Tracked

Interface	Description
Async	Asynchronous interface
BVI	Bridge-Group Virtual Interface
CDMA-Ix	CDMA Ix interface
CTunnel	CTunnel interface
Dialer	Dialer interface
FastEthernet	FastEthernet IEEE 802.3
Lex	Lex interface
Loopback	Loopback interface
MFR	Multilink Frame Relay bundle intrface
Multilink	Multilink-group interface
Null	Null interface
Port-channel	Ethernet channel of interfaces
Serial	Serial
Tunnel	Tunnel interface

Table 145 Interfaces That Can Be Tracked (continued)

Interface	Description
vif	Pragmatic General Multicast (PGM) multicast host interface
virtual	Virtual interface
virtual-PPP	Virtual PPP interface
virtual-Template	Virtual template interface
virtual-TokenRing	Virtual TokenRing
XTagATM	Extended Tag ATM interface

Examples

The following example shows that all host entries are to be tracked:

```
Router# show ip device tracking all count

IP Device Tracking = Enabled
Probe Count: 2
Probe Interval: 10
```

The fields in the above display are self-explanatory.

show ip inspect

To display Context-Based Access Control (CBAC) configuration and session information, use the **show ip inspect** command in privileged EXEC mode.

ACL Bypass Statistics Syntax

show ip inspect {**name** *inspection-name* | **config** | **interfaces** | **sessions** [**detail**] | **statistics** [**reset**] | **all** | **sis** [**detail**] | **tech-support** [**reset**]} [**vrf** *vrf-name*]

Firewall MIB Statistics Syntax

show ip inspect mib connection-statistics {**global** | **l4-protocol** {**all** | **icmp** | **tcp** | **udp**} | **l7-protocol** [*protocol-type*] | **policy** *policy-name* **interface** [*interface-type interface-number*] {**l4-protocol** {**all** | **icmp** | **tcp** | **udp**} | **l7-protocol** [*protocol-type*]}

Syntax Description

name *inspection-name*	Displays the configured inspection rule with the name *inspection-name*.
config	Displays the complete CBAC or High Availability (HA) inspection configuration.
interfaces	Displays the interface configuration with respect to applied inspection rules and access lists.
sessions [**detail**]	Displays existing sessions that are currently being tracked and inspected by CBAC or HA. The optional **detail** keyword allows additional details about these sessions to be shown.
statistics [**reset**]	Displays CBAC session statistics, such as the number of TCP and HTTP packets that are processed through the inspection, the number of sessions that have been created since the subsystem startup, the current session count, the maximum session count, and the session creation rate. The optional **reset** keyword resets the counters to reflect the latest statistics.
all	Displays all CBAC configuration and all existing sessions that are currently being tracked and inspected by CBAC.
sis [**detail**]	Displays CBAC session information such as window-size information of initiator and responder windows in a session. The optional **detail** keyword allows additional details about these sessions to be shown.
tech-support [**reset**]	Displays additional information regarding drops that are not shown in the **show ip inspect statistics** command. This information is useful for troubleshooting IP inspect issues. The optional **reset** keyword resets the counters to reflect the latest statistics.
vrf *vrf-name*	(Optional) Displays information only for the specified Virtual Routing and Forwarding (VRF) interface.
mib connection-statistics	Displays firewall performance summary statistics that are monitored via firewall MIBs.
global	Displays global connection summary statistics, which are kept for the entire device.
l4-protocol	Displays Layer 4 protocol-based connection summary statistics. Valid values include **all**, **icmp**, **tcp**, **udp**.

l7-protocol [*protocol-type*]	Displays Layer 7 protocol-based connection summary statistics. Refer to Table 146 for the protocols that can be entered for the *protocol-type* argument.
policy *policy-name*	Displays the name of the firewall policy that is being monitored.
interface	Displays the type of the interface on which the specified firewall policy is applied.
interface-type	Interface type. For more information, use the question mark (?) online help function.
interface-number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2 P	This command was introduced.
12.3(4)T	This command was modified. The output for the **show ip inspect session detail** command was enhanced to support dynamic access control list (ACL) bypass.
12.3(11)T	This command was modified. The **statistics** keyword was added.
12.3(14)T	This command was modified. The output shows the IMAP and POP3 configuration. The **vrf** *vrf-name* keyword/argument pair was added.
12.4(6)T	This command was modified. • The firewall MIB statistics syntax was added to support firewall performance via SNMP. • High Availability (HA) configuration and session information was added to support Stateful Failover.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.4(11)T	This command was modified. The **tech-support** and **sis** keywords were unhidden and are now supported.
12.2SX	This command was integrated into Cisco IOS Release 12.2SX. Support in a specific 12.2SX release depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to view the CBAC and HA configuration and session information.

ACL Bypass Functionality

ACL bypass allows a packet to avoid redundant ACL checks by allowing the firewall to permit the packet on the basis of existing inspection sessions instead of dynamic ACLs. Because input and output dynamic ACLs have been eliminated from the firewall configuration, the **show ip inspect session detail** command output no longer shows dynamic ACLs. Instead, the output displays the matching inspection session for each packet that is permitted through the firewall.

Firewall MIB Functionality

The Cisco Unified Firewall MIB monitors the following firewall performance statistics:

- Connection statistics, which are a record of the firewall traffic streams that have attempted to flow through the firewall system. Connection statistics can be displayed on a global basis, a protocol-specific basis, or a firewall policy basis.
- URL filtering statistics, which include the status of distinct URL filtering servers that are configured on the firewall and the impact of the performance of the URL filtering servers on the latency and throughput of the firewall.

Table 146 shows the types of protocols that can be configured for the *protocol-type* argument with the **l7-protocol** keyword:

Table 146 Protocol Types for the l7-protocol Keyword

Protocol-Type	Description
802-11-iapp	IEEE 802.11 WLANs WG IAPP
ace-svr	ACE Server/Propagation
all	All protocols
aol	America Online Instant Messenger
appleqtc	Apple QuickTime
bgp	Border Gateway Protocol
biff	Bliff Mail Notification
bootpc	Bootstrap Protocol Client
bootps	Bootstrap Protocol Server
cddbp	CD Database Protocol
cifs	CIFS
cisco-fna	Cisco FNATIVE
cisco-net-mgmt	Cisco Network Management
cisco-svcs	Cisco license/perf/GDP/X.25/ident svcs
cisco-sys	Cisco SYSMAINT
cisco-tdp	Cisco Tag Distribution Protocol
cisco-tna	Cisco TNATIVE
citrix	Citrix IMA/ADMIN/RTMP
citirixmaclient	Citrix IMA Client
clp	Cisco Line Protocol
creativepartnr	Creative Partner
creativeserver	Creative Server
cuseeme	CUSeeMe Protocol
daytime	Daytime Protocol (RFC 867)
dbase	dBASE Unix
dbcontrol_agent	Oracle Database Control Agent
ddns-v3	Dynamic Domain Name Server Version 3

Table 146 Protocol Types for the l7-protocol Keyword

Protocol-Type	Description
dhcp-failover	Dynamic Host Control Protocol failover
discard	Discard Protocol
dns	Domain Name Server
dnsix	DNSIX Security Attribute Token Map
echo	Echo Protocol
entrust-svc-hdlr	Entrust KM/Admin Service Handler
entrust-svcs	Entrust sps/aaas/aams
exec	Remote Process Execution
fcip-port	Fibre Channel over IP
finger	Finger Protocol
ftp	File Transfer Protocol
ftps	File Transfer Protocol over Transport Layer Security/ Secure Sockets Layer
gdoi	Group Domain of Interpretation
giop	Oracle GIOP/SSL
gopher	Gopher Protocol
gtpv0	GPRS Tunneling Protocol Version 0
gtpv1	GPRS Tunneling Protocol Version 1
h323	H.323 Protocol for audio-visual communication
h323-annexe	H.323 Protocol AnnexE
h323-nxg	H.323 Protocol AnnexG
hp-alarm-mgr	HP Performance Data Alarm Manager
hp-collector	HP Performance Data Collector
hp-managed-node	HP Performance Data Managed Node
hsrp	Hot Standby Router Protocol
http	Hyper Text Transfer Protocol
https	Secure Hyper Text Transfer Protocol
ica	ICA from Citrix
icabrowser	ICA browser from Citrix
ident	Ident Protocol
igmpv3lite	Internet Group Management Protocol over User Datagram Protocol for SSM
imap	Internet Message Access Protocol
imap3	Interactive Mail Access Protocol 3
imaps	IMAP over TLS/SSL
ipass	IPASS
ipsec-msft	Microsoft IPsec NAT-T

Table 146 Protocol Types for the l7-protocol Keyword

Protocol-Type	Description
ipx	IPX
irc	Internet Relay Chat Protocol
ircs	IRC over TLS/SSL
irc-serv	IRC Serv
ircu	IRCU
isakmp	Internet Security Association and Key Management Protocol
iscsi	Internet Small Computer System Interface
iscsi-target	iSCSI Port
kerberos	Kerberos Protocol
kermit	Kermit Protocol
l2tp	Layer 2 Tunneling Protocol
ldap	Lightweight Directory Access Protocol
ldap-admin	LDAP admin server port
ldaps	LDAP over TLS/SSL
login	Remote Login
lotusmtap	Lotus Mail Tracking Agent Protocol
lotusnotes	Lotus Note
mgcp	Media Gateway Control Protocol
microsoft-ds	Microsoft DS
ms-cluster-net	Microsoft Cluster Net
ms-dotnetster	Microsoft .NETster Port
ms-sna	Microsoft SNA Server/Base
ms-sql	Microsoft SQL
ms-sql-m	Microsoft SQL Monitor
msexch-routing	Microsoft Exchange Routing
msnmsgr	MSN Instant Messenger
msrpc	Microsoft Remote Procedure Call
mysql	MySQL
n2h2server	N2H2 Filter Service Port
ncp	NetWare Core Protocol
net8-cman	Oracle Net8 Cman/Admin
netbios-dgm	NETBIOS Datagram Service
netbios-ns	NETBIOS Name Service
netbios-ssn	NETBIOS Session Service
netshow	Microsoft NetShow

Table 146 Protocol Types for the l7-protocol Keyword

Protocol-Type	Description
netstat	Network Statistics
nfs	Network File System
nntp	Network News Transport Protocol
ntp	Network Time Protocol
oem-agent	Oracle Enterprise Manager Agent
oracle	Oracle
oracle-em-vp	Oracle Enterprise Manager/VP
oraclenames	Oracle Names
orasrv	Oracle SQL *NET Version 1/2
other	Non-listed Protocols
pcanywheredata	pcAnywhere data
pcanywherestat	pcAnywhere stat
pop3	Post Office Protocol Version 3
pop3s	POP3 over TLS/SSL
pptp	Point-to-Point Tunneling Protocol
pwdgen	Password Generator Protocol
qmtp	Quick Mail Transfer Protocol
radius	RADIUS and Accounting
rdb-dbs-disp	Oracle Relational Database
realmedia	Real Network's Realmedia Protocol
realsecure	ISS Real Secure Console Service Port
router	Local Routing Process
rsvd	RSVD
rsvp-encap	RSVP Encapsulation-1/2
rsvp_tunnel	RSVP Tunnel
rtc-pm-port	Oracle RTC-PM Port
rtelnet	Remote Telnet Service
rtsp	Real Time Streaming Protocol
r-winsock	Remote Winsock
send	SEND
shell	Remote Command
sip	Session Initiation Protocol
sip-tls	SIP-TLS
skinny	Skinny Client Control Protocol
sms	SMS
smtp	Simple Mail Transfer Protocol

Table 146 Protocol Types for the l7-protocol Keyword

Protocol-Type	Description
snmp	Simple Network Management Protocol
snmptrap	SNMP Trap
socks	Socks
sql-net	SQL-NET
sqlserv	SQL Services
sqlsrv	SQL Service
ssh	SSH Remote Login Protocol
sshell	SSLshell
ssp	State Sync Protocol
streamworks	StreamWorks Protocol
stun	Cisco STUN
sunrpc	SUN Remote Procedure Call
syslog	Syslog Service
syslog-conn	Reliable Syslog Service
tacacs	Terminal Access Controller Access-Control System
tacacs-ds	TACACS Database Service
tarantella	Tarantella
telnet	Telecommunication Network Protocol.
telnets	Telnet over TLS or SSL
tftp	Trivial File Transfer Protocol
time	Time
timed	Time Server
tr-rsrb	Cisco RSBR
ttc	Oracle TTC or SSL
uucp	Unix-to-Unix Copy Program
vdolive	VDOLive Protocol
vqp	VLAN Query Protocol
webster	Webster Network dictionary
who	Who’s Service
wins	Windows Internet Name Service
x11	X Window System
xdmcp	XDM Control Protocol
ymsgr	Yahoo Instant Messenger

Examples

The following is sample output for the **show ip inspect name myinspectionrule** command, where the inspection rule "myinspectionrule" is configured. In this example, the output shows the protocols that should be inspected by CBAC and the corresponding idle timeouts for each protocol.

```
Router# show ip inspect name myinspectionrule

Inspection Rule Configuration
 Inspection name myinspectionrule
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
```

The following is sample output from the **show ip inspect config** command. In this example, the output shows CBAC configuration, including global timeouts, thresholds, and inspection rules.

```
Router# show ip inspect config

Session audit trail is disabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
 Inspection name myinspectionrule
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
```

The following is sample output from the **show ip inspect interfaces** command:

```
Router# show ip inspect interfaces

Interface Configuration
 Interface Ethernet0
  Inbound inspection rule is myinspectionrule
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
  Outgoing inspection rule is not set
  Inbound access list is not set
  Outgoing access list is not set
```

The following is sample output from the **show ip inspect sessions** command. In this example, the output shows the source and destination addresses and port numbers (separated by colons), and it indicates that the session is an FTP session.

```
Router# show ip inspect sessions

Established Sessions
 Session 25A3318 (10.0.0.1:20)=>(10.1.0.1:46068) ftp-data SIS_OPEN
 Session 25A6E1C (10.1.0.1:46065)=>(10.0.0.1:21) ftp SIS_OPEN
```

The following is sample output from the **show ip inspect all** command:

```
Router# show ip inspect all

Session audit trail is disabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
```

```
dns-timeout is 5 sec
Inspection Rule Configuration
 Inspection name all
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
Interface Configuration
 Interface Ethernet0
  Inbound inspection rule is all
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
  Outgoing inspection rule is not set
  Inbound access list is not set
  Outgoing access list is not set
 Established Sessions
 Session 25A6E1C (10.3.0.1:46065)=>(10.4.0.1:21) ftp SIS_OPEN
 Session 25A34A0 (10.4.0.1:20)=>(10.3.0.1:46072) ftp-data SIS_OPEN
```

The following is sample output from the **show ip inspect session detail** command, which shows that an outgoing ACL and an inbound ACL (dynamic ACLs) have been created to allow return traffic:

```
Router# show ip inspect session detail

Established Sessions
 Session 80E87274 (192.168.1.116:32956)=>(192.168.101.115:23) tcp SIS_OPEN
   Created 00:00:08, Last heard 00:00:04
   Bytes sent (initiator:responder) [140:298] acl created 2
   Outgoing access-list 102 applied to interface FastEthernet0/0
   Inbound access-list 101 applied to interface FastEthernet0/1
```

The following is sample output from the **show ip inspect session detail** command, which shows related ACL information (such as session identifiers [SIDs]), but does not show dynamic ACLs, which are no longer created:

```
Router# show ip inspect session detail

Established Sessions
 Session 814063CC (192.168.1.116:32955)=>(192.168.101.115:23) tcp SIS_OPEN
  Created 00:00:10, Last heard 00:00:06
  Bytes sent (initiator:responder) [140:298]
  HA state: HA_STANDBY
  In  SID 192.168.101.115[23:23]=>192.168.1.117[32955:32955] on ACL 101 (15 matches)
  Out SID 192.168.101.115[23:23]=>192.168.1.116[32955:32955] on ACL 102
```

The following is sample output from the **show ip inspect statistics** command:

```
Router# show ip inspect statistics

Packet inspection statistics [process switch:fast switch]
  tcp packets: [616668:0]
  http packets: [178912:0]
Interfaces configured for inspection 1
Session creations since subsystem startup or last reset 42940
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [98:68:50]
Last session created 5d21h
Last statistic reset never
Last session creation rate 0
Last half-open session total 0
```

The following is sample output from the **show ip inspect tech-support** command:

```
Router# show ip inspect tech-support
```

```
Packet inspection statistics [process switch:fast switch]
  tcp packets: [21:879]
Interfaces configured for inspection 1 Pre-gen sessions 0
Session creations since subsystem startup or last reset 19
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [1:1:1]
Last session created 02:25:37
Last statistic reset never
Last session creation rate 0
Last half-open session total 0

Packet disposition statistics [process switch:fastswitch]
  tcp packets dropped: [1:3]
  tcp packets skipped: [0:35]
TCP session reset: 0
```

The following is sample output from the **show ip inspect sis detail** command:

```
Router# show ip inspect sis detail

 Half-open Sessions
 Session 459B498 (75.75.75.3:25471)=>(10.10.10.3:5060) tcp SIS_OPENING
 Created 00:00:01, Last heard 00:00:01
 Bytes sent (initiator:responder) [0:0]
 Initiator->Responder Window size 8000 Scale factor 0
 Responder->Initiator Window size 0 Scale factor 0
Router#
```

The following is sample output from the **show ip inspect mib** command with global or protocol-specific keywords.

Global MIB Statistics

```
Router# show ip inspect mib connection-statistics global

Connections Attempted 7
Connections Setup Aborted 0
Connections Policy Declined 0
Connections Resource Declined 0
Connections Half Open 2
Connections Active 3
Connections Expired 2
Connections Aborted 0
Connections Embryonic 0
Connections 1-min Setup Rate 5
Connections 5-min Setup Rate 7
```

Protocol-Based MIB Statistics

```
Router# show ip inspect mib connection-statistics l4-protocol tcp

Protocol tcp
Connections Attempted 3
Connections Setup Aborted 0
Connections Policy Declined 0
Connections Resource Declined 0
Connections Half Open 1
Connections Active 2
Connections Aborted 0
Connections 1-min Setup Count 3
Connections 5-min Setup Count 3
```

```
Router# show ip inspect mib connection-statistics l7-protocol http

Protocol http
Connections Attempted 3
Connections Setup Aborted 0
Connections Policy Declined 2
Connections Resource Declined 0
Connections Half Open 0
Connections Active 1
Connections Aborted 0
Connections 1-min Setup Rate 1
Connections 5-min Setup Rate 2
```

Policy-target-Based MIB Statistics

```
Router# show ip inspect mib connection-statistics policy ftp interface GigabitEthernet0/0
l4-protocol tcp

! Policy Target Protocol Based Connection Summary Stats

Policy ftp-inspection
Target GigabitEthernet0/0
Protocol tcp
Connections Attempted 3
Connections Setup Aborted 0
Connections Policy Declined 0
Connections Resource Declined 0
Connections Half Open 1
Connections Active 2
Connections Aborted 0

Router# show ip inspect mib connection-statistics policy ftp interface GigabitEthernet0/0
l7-protocol ftp

! Policy Target Protocol Based Connection Summary Stats
Policy ftp-inspection
Target GigabitEthernet0/0
Protocol ftp
Connections Attempted 3
Connections Setup Aborted 0
Connections Policy Declined 0
Connections Resource Declined 0
Connections Half Open 1
Connections Active 2
Connections Aborted 0
```

show ip inspect ha

To display stateful failover high availability (HA) session information, use the **show ip inspect ha** command in privileged EXEC mode.

show ip inspect ha [**sessions** [**detail**] [**vrf** *vrf-name*] | **statistics**]

Syntax Description

sessions	(Optional) Displays information about the sessions.
detail	(Optional) Displays additional information on pinholes created for the return traffic, number of bytes that have passed through this session, and session time information.
vrf *vrf-name*	(Optional) Displays information for the specified virtual routing and forwarding (VRF) instance.
statistics	(Optional) Displays HA sessions statistics for both the active and standby devices.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following is sample output from the **show ip inspect ha sessions** command.

```
Router# show ip inspect ha sessions

Sess_ID  (src_addr:port)=>(dst_addr:port)  proto  sess_state ha_state  Established Session
2CA8958 (10.0.0.5:37690)=>(10.0.0.4:00023) tcp    SIS_OPEN   HA_ACTIVE
```

Table 142 describes the significant fields shown in the display.

Table 147 show ip inspect ha sessions Field Descriptions

Field	Description
Sess_ID	Displays the session ID.
src_addr:port	Displays source address and port.
dst_addr:port	Displays the destination address and port.
proto	Displays the name of the protocol.
sess_state	Displays the session state.
ha_state	Displays the HA state.
Established Session	Displays the name of the established session.

The following sample output from the **show ip inspect ha sessions detail** command displays additional information for each session.

```
Router# show ip inspect ha sessions detail

Sess_ID  (src_addr:port)=>(dst_addr:port)  proto  sess_state ha_state  Established Session
2CA8958 (10.0.0.5:37690)=>(10.0.0.4:00023) tcp    SIS_OPEN   HA_ACTIVE
 Created 00:01:52, Last heard 00:01:39
 Bytes sent (initiator:responder) [50:91]
 In  SID   10.11.0.4[23:23]=>10.0.0.5[37690:37690] on ACL test  (25 matches)
```

Table 148 describes the significant fields shown in the display.

Table 148 show ip inspect ha sessions detail Field Descriptions

Field	Description
Created	Displays the date the session was created.
Last heard	Displays the date the packets were received last on the session.
Bytes sent (initiator:responder)	Displays the ratio of bytes sent from the initiator to the responder.
In SID	Session identifier.
on ACL test	Session identifier entry open on an Access Control List (ACL) named test.

The following sample output from the **show ip inspect ha statistics** command displays the following information for the session on the active and standby routers.

On the active router:

```
Router # show ip inspect ha statistics

**************************************************
FW HA ACTIVE STATS
**************************************************
FW HA active num add session sent            1
FW HA active num delete session sent         0
FW HA active num update session requests     0
FW HA active num update session sent         17
FW HA active bulk sync session               0
FW HA active num error                       0
FW HA active RF error                        0
FW HA active CF error                        0
FW HA active manager error                   0
**************************************************
```

On the standby router:

```
Router # show ip inspect ha statistics

**************************************************
FW HA STANDBY STATS
**************************************************
FW HA standby num add session received       1
FW HA standby num delete session received    0
FW HA standby num update session received    17
FW HA standby num bulk sync request sent     0
FW HA standby num error                      0
FW HA standby config error                   0
**************************************************
```

Table 149 describes the significant fields shown in the display.

Table 149 show ip inspect ha Field Descriptions

Field	Description
num add session sent	Displays the number of add session messages sent.
num delete session sent	Displays the number of delete session messages sent.
num update session requests	Displays the number of update session message requests.
num update session sent	Displays the number of update session messages sent.
bulk sync session	Displays the number of bulk synchronization requests received.
num error	Displays the number of errors.
RF error	Displays the number of Redundancy Framework (RF) errors.
CF error	Displays the number of Checkpointing Facility (CF) errors.
manager error	Displays the number of manager errors.
bulk sync request sent	Displays the number of bulk synchronization requests sent.
config error	Displays the number of configuration errors.

Related Commands

Command	Description
show ip inspect	Displays CBAC configuration and session information.

show ip interface

To display the usability status of interfaces configured for IP, use the **show ip interface** command in privileged EXEC mode.

show ip interface [*type number*] [**brief**]

Syntax Description

type	(Optional) Interface type.
number	(Optional) Interface number.
brief	(Optional) Displays a summary of the usability status information for each interface.

Command Default

The full usability status is displayed for all interfaces configured for IP.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(3)T	The command output was modified to show the status of the **ip wccp redirect out** and **ip wccp redirect exclude add in** commands.
12.2(14)S	The command output was modified to display the status of NetFlow on a subinterface.
12.2(15)T	The command output was modified to display the status of NetFlow on a subinterface.
12.3(6)	The command output was modified to identify the downstream VPN routing and forwarding (VRF) instance in the output.
12.3(14)YM2	The command output was modified to show the usability status of interfaces configured for Multiprocessor Forwarding (MPF) and implemented on the Cisco 7301 and Cisco 7206VXR routers.
12.2(14)SX	This command was implemented on the Supervisor Engine 720.
12.2(17d)SXB	This command was integrated into Cisco IOS 12.2(17d)SXB on the Supervisor Engine 2, and the command output was changed to include NDE for hardware flow status.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	The command output was modified to display information about the Unicast Reverse Path Forwarding (RPF) notification feature.
12.4(20)T	The command output was modified to display information about the Unicast RPF notification feature.

Release	Modification
12.2(33)SXI2	This command was modified. The command output was modified to display information about the Unicast RPF notification feature.
Cisco IOS XE Release 2.5	This command was modified. This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The Cisco IOS software automatically enters a directly connected route in the routing table if the interface is usable (which means that it can send and receive packets). If an interface is not usable, the directly connected routing entry is removed from the routing table. Removing the entry lets the software use dynamic routing protocols to determine backup routes to the network, if any.

If the interface can provide two-way communication, the line protocol is marked "up." If the interface hardware is usable, the interface is marked "up."

If you specify an optional interface type, information for that specific interface is displayed. If you specify no optional arguments, information on all the interfaces is displayed.

When an asynchronous interface is encapsulated with PPP or Serial Line Internet Protocol (SLIP), IP fast switching is enabled. A **show ip interface** command on an asynchronous interface encapsulated with PPP or SLIP displays a message indicating that IP fast switching is enabled.

You can use the **show ip interface brief** command to display a summary of the router interfaces. This command displays the IP address, the interface status, and other information.

The **show ip interface brief** command does not display any information related to Unicast RPF.

Examples

The following example shows configuration information for interface Gigabit Ethernet 0/3. In this example, the IP flow egress feature is configured on the output side (where packets go out of the interface), and the policy route map named PBRNAME is configured on the input side (where packets come into the interface).

```
Router# show running-config interface gigabitethernet 0/3

interface GigabitEthernet0/3
 ip address 10.1.1.1 255.255.0.0
 ip flow egress
 ip policy route-map PBRNAME
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
end
```

The following example shows interface information on Gigabit Ethernet interface 0/3. In this example, MPF is enabled, and both Policy Based Routing (PBR) and NetFlow features are not supported by MPF and are ignored.

```
Router# show ip interface gigabitethernet 0/3

GigabitEthernet0/3 is up, line protocol is up
  Internet address is 10.1.1.1/16
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
```

```
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Feature Fast switching turbo vector
  IP VPN Flow CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is enabled, using route map PBR
  Network address translation is disabled
  BGP Policy Mapping is disabled
  IP Multi-Processor Forwarding is enabled
     IP Input features, "PBR",
         are not supported by MPF and are IGNORED
     IP Output features, "NetFlow",
         are not supported by MPF and are IGNORED
```

The following example identifies a downstream VRF instance. In the example, “Downstream VPN Routing/Forwarding “D”” identifies the downstream VRF instance.

```
Router# show ip interface virtual-access 3

Virtual-Access3 is up, line protocol is up
  Interface is unnumbered. Using address of Loopback2 (10.0.0.8)
  Broadcast address is 255.255.255.255
  Peer address is 10.8.1.1
  MTU is 1492 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is enabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Feature Fast switching turbo vector
  IP VPN CEF switching turbo vector
  VPN Routing/Forwarding "U"
  Downstream VPN Routing/Forwarding "D"
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
```

```
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

The following example shows the information displayed when Unicast RPF drop-rate notification is configured:

```
Router# show ip interface ethernet 2/3

Ethernet2/3 is up, line protocol is up
  Internet address is 10.0.0.4/16
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP Flow switching is disabled
  IP CEF switching is disabled
  IP Null turbo vector
  IP Null turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are No CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

Unicast RPF Information

```
  Input features: uRPF
  IP verify source reachable-via RX, allow default
   0 verification drops
   0 suppressed verification drops
   0 verification drop-rate
Router#
```

The following example shows how to display the usability status for a specific VLAN:

```
Router# show ip interface vlan 1

Vlan1 is up, line protocol is up
  Internet address is 10.0.0.4/24
  Broadcast address is 255.255.255.255
Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Fast switching turbo vector
  IP Normal CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
  Sampled Netflow is disabled
  IP multicast multilayer switching is disabled
  Netflow Data Export (hardware) is enabled
```

Table 150 describes the significant fields shown in the display.

Table 150 show ip interface Field Descriptions

Field	Description
Virtual-Access3 is up	Shows whether the interface hardware is usable (up). For an interface to be usable, both the interface hardware and line protocol must be up.
Broadcast address is	Broadcast address.
Peer address is	Peer address.
MTU is	MTU value set on the interface, in bytes.
Helper address	Helper address, if one is set.
Directed broadcast forwarding	Shows whether directed broadcast forwarding is enabled.
Outgoing access list	Shows whether the interface has an outgoing access list set.

Table 150 show ip interface Field Descriptions (continued)

Field	Description
Inbound access list	Shows whether the interface has an incoming access list set.
Proxy ARP	Shows whether Proxy Address Resolution Protocol (ARP) is enabled for the interface.
Security level	IP Security Option (IPSO) security level set for this interface.
Split horizon	Shows whether split horizon is enabled.
ICMP redirects	Shows whether redirect messages will be sent on this interface.
ICMP unreachables	Shows whether unreachable messages will be sent on this interface.
ICMP mask replies	Shows whether mask replies will be sent on this interface.
IP fast switching	Shows whether fast switching is enabled for this interface. It is generally enabled on serial interfaces, such as this one.
IP Flow switching	Shows whether Flow switching is enabled for this interface.
IP CEF switching	Shows whether Cisco Express Forwarding switching is enabled for the interface.
Downstream VPN Routing/Forwarding "D"	Shows the VRF instance where the PPP peer routes and AAA per-user routes are being installed.
IP multicast fast switching	Shows whether multicast fast switching is enabled for the interface.
IP route-cache flags are Fast	Shows whether NetFlow is enabled on an interface. Displays "Flow init" to specify that NetFlow is enabled on the interface. Displays "Ingress Flow" to specify that NetFlow is enabled on a subinterface using the **ip flow ingress** command. Shows "Flow" to specify that NetFlow is enabled on a main interface using the **ip route-cache flow** command.
Router Discovery	Shows whether the discovery process is enabled for this interface. It is generally disabled on serial interfaces.
IP output packet accounting	Shows whether IP accounting is enabled for this interface and what the threshold (maximum number of entries) is.
TCP/IP header compression	Shows whether compression is enabled.
WCCP Redirect outbound is disabled	Shows the status of whether packets received on an interface are redirected to a cache engine. Displays "enabled" or "disabled."
WCCP Redirect exclude is disabled	Shows the status of whether packets targeted for an interface will be excluded from being redirected to a cache engine. Displays "enabled" or "disabled."
Netflow Data Export (hardware) is enabled	NetFlow Data Expert (NDE) hardware flow status on the interface.

The following example shows how to display a summary of the usability status information for each interface:

```
Router# show ip interface brief

Interface     IP-Address     OK?  Method  Status                  Protocol
Ethernet0     10.108.00.5    YES  NVRAM   up                      up
Ethernet1     unassigned     YES  unset   administratively down   down
Loopback0     10.108.200.5   YES  NVRAM   up                      up
Serial0       10.108.100.5   YES  NVRAM   up                      up
Serial1       10.108.40.5    YES  NVRAM   up                      up
Serial2       10.108.100.5   YES  manual  up                      up
Serial3       unassigned     YES  unset   administratively down   down
```

Table 151 describes the significant fields shown in the display.

Table 151 show ip interface brief Field Descriptions

Field	Description
Interface	Type of interface.
IP-Address	IP address assigned to the interface.
OK?	"Yes" means that the IP Address is valid. "No" means that the IP Address is not valid.
Method	The Method field has the following possible values: • RARP or SLARP—Reverse Address Resolution Protocol (RARP) or Serial Line Address Resolution Protocol (SLARP) request. • BOOTP—Bootstrap protocol. • TFTP—Configuration file obtained from the TFTP server. • manual—Manually changed by the command-line interface. • NVRAM—Configuration file in NVRAM. • IPCP—**ip address negotiated** command. • DHCP—**ip address dhcp** command. • unassigned—No IP address. • unset—Unset. • other—Unknown.
Status	Shows the status of the interface. Valid values and their meanings are: • up—Interface is up. • down—Interface is down. • administratively down—Interface is administratively down.
Protocol	Shows the operational status of the routing protocol on this interface.

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
ip vrf autoclassify	Enables VRF autoclassify on a source interface.
match ip source	Specifies a source IP address to match to required route maps that have been set up based on VRF connected routes.
route-map	Defines the conditions for redistributing routes from one routing protocol into another or to enable policy routing.
set vrf	Enables VPN VRF selection within a route map for policy-based routing VRF selection.
show ip arp	Displays the ARP cache, in which SLIP addresses appear as permanent ARP table entries.
show route-map	Displays static and dynamic route maps.

show ip ips

To display Intrusion Prevention System (IPS) information such as configured sessions and signatures, use the **show ip ips** command in privileged EXEC mode.

Note Effective with Cisco IOS Release 15.1(4)M, the Cisco Services for IPS on IOS feature is not available in Cisco IOS software. As a result, the **license** keyword was removed from this command.

show ip ips {**all** | **configuration** | **interfaces** | **license** | **name** *name* | **sessions** [**detail**] [**vrf** *vrf-name*] | **signatures** [[**count**] [**detail** | **engine** [*engine-name*] | **sigid** [*sigid* [**subid** [*subid*]]]] | [**statistics**]] | **statistics** [**reset**] [**vrf** *vrf-name*]}

Syntax Description

all	Displays all available IPS information.
configuration	Displays additional configuration information, including default values that may not be displayed using the **show running-config** command.
interfaces	Displays the interface configuration.
license	Displays license and signature package information.
name *name*	Displays information only for the specified IPS rule.
sessions	Displays IPS session-related information.
detail	(Optional) Shows detailed session information.
vrf *vrf-name*	(Optional) Shows detailed session and latest statistics information per user specific VRF.
signatures	Displays signature information, such as which signatures are disabled and marked for deletion.
count	(Optional) Displays the number of signatures enabled, retired, and compiled.
detail	(Optional) Displays detailed signature information.
engine *engine-name*	(Optional) Displays signatures of a selected engine.
sigid *sigid*	(Optional) Displays signature ID for selected signatures.
subid *subid*	(Optional) Displays the sub ID for selected signatures.
statistics	(Optional) Displays the information such as the number of packets audited and the number of alarms sent.
statistics	Displays the information such as the number of packets audited and the number of alarms sent.
reset	(Optional) Resets sample output to reflect the latest statistics.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	This command was modified. The command name was changed from **show ip audit** to **show ip ips**. Also, all **show ip ips** commands were combined into a single command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
12.4(20)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.4(22)T	This command was modified. The **count**, **detail**, **engine**, **sigid**, **signatures**, and **subid** keywords and the *engine-name*, *subid*, and *sigid* arguments were added.
15.0(1)M	This command was modified. The **license** keyword was added.
15.1(4)M	This command was modified. The **license** keyword was removed.

Usage Guidelines

Use the **show ip ips configuration** command to display additional configuration information, including default values that may not be displayed using the **show running-config** command.

Examples

Sample Output for the show ip ips configuration Command

The following example displays the output of the **show ip ips configuration** command:

```
Router# show ip ips configuration
Event notification through syslog is enabled
Event notification through Net Director is enabled
Default action(s) for info signatures is alarm
Default action(s) for attack signatures is alarm
Default threshold of recipients for spam signature is 25
PostOffice:HostID:5 OrgID:100 Addr:10.2.7.3 Msg dropped:0
HID:1000 OID:100 S:218 A:3 H:14092 HA:7118 DA:0 R:0
    CID:1 IP:172.21.160.20 P:45000 S:ESTAB (Curr Conn)

Audit Rule Configuration
 Audit name AUDIT.1
    info actions alarm
```

Sample Output for the show ip ips interfaces Command

The following example displays the output of the **show ip ips interfaces** command:

```
Router# show ip ips interfaces
Interface Configuration
 Interface Ethernet0
  Inbound IPS audit rule is AUDIT.1
    info actions alarm
  Outgoing IPS audit rule is not set
 Interface Ethernet1
  Inbound IPS audit rule is AUDIT.1
    info actions alarm
  Outgoing IPS audit rule is AUDIT.1
    info actions alarm
```

Sample Output for the show ip ips statistics Command

The following example displays the output of the **show ip ips statistics** command:

```
Router# show ip ips statistics
Signature audit statistics [process switch:fast switch]
  signature 2000 packets audited: [0:2]
  signature 2001 packets audited: [9:9]
  signature 2004 packets audited: [0:2]
  signature 3151 packets audited: [0:12]
Interfaces configured for audit 2
Session creations since subsystem startup or last reset 11
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [2:1:0]
Last session created 19:18:27
Last statistic reset never

HID:1000 OID:100 S:218 A:3 H:14085 HA:7114 DA:0 R:0
```

Sample Output for the show ip ips statistics vrf Command

The following example displays the output of the **show ip ips statistics vrf** *vrf-name* command:

```
Router# show ip ips statistics vrf VRF_600
Signature statistics [process switch:fast switch]
  signature 5170:1 packets checked: [0:2]
Interfaces configured for ips 3
Session creations since subsystem startup or last reset 4
Current session counts (estab/half-open/terminating) [1:0:0]
Maxever session counts (estab/half-open/terminating) [2:1:1]
Last session created 00:02:34
Last statistic reset never
TCP reassembly statistics
  received 8 packets out-of-order; dropped 0
  peak memory usage 12 KB; current usage: 0 KB
  peak queue length 6
```

Sample Output for the show ip ips sessions vrf Command

The following example displays the output of the **show ip ips sessions vrf** *vrf-name* command:

```
Router# show ip ips sessions vrf VRF_600
Established Sessions
 Session 67D5C744 (10.0.4.2:34000)=>(10.0.6.2:23) tcp SIS_OPEN
```

Sample Output for the show ip ips license Command

The following example displays the output of the **show ip ips license** command:

```
Router# show ip ips license
IPS License Status Valid
Expiration Date: 2009-12-31
Signatures Loaded: 2009-06-25 S375
Signature Package: 2009-06-25 S375
```

The sample output shows the details for a valid IPS license. Note the license expiration date (2009-12-31), the version date of the existing S375 loaded signatures (2009-07-24 S375), and the version date of the last signature package (S375) loaded (2009-07-24 S375). The license is valid as the existing loaded signature version date is the same as the last signature package version date. The last signature package date (2009-07-24) is also before the license expiration date (2009-12-31).

Related Commands

Command	Description
clear ip ips statistics	Resets statistics on packets analyzed and alarms sent.

show ip ips auto-update

To display the automatic signature update configuration, use the **show ip ips auto-update** command in EXEC mode.

show ip ips auto-update

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Automatic signature updates allow users to override the existing Intrusion Prevention System (IPS) configuration and automatically keep signatures up to date on the basis of a preset time, which can be configured to a preferred setting.

Use the **show ip ips auto-update** command to verify the auto update configuration.

Examples

The following example shows how to configure automatic signature updates and issue the **show ip ips auto-update** command to verify the configuration. In this example, the signature package file is pulled from the TFTP server at the start of every hour or every day, Sunday through Thursday. (Note that adjustments are made for months without 31 days and daylight savings time.)

```
Router# clock set ?
   hh:mm:ss Current Time
Router# clock set 10:38:00 20 apr 2006
Router#
*Apr 20 17:38:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 10:37:55 MST
Thu Apr 20 2006 to 10:38:00 MST Thu Apr 20 2006, configured from console by cisco on
console.

Router(config)# ip ips auto-update
Router(config-ips-auto-update)# occur-at 0 0-23 1-31 1-5
Router(config-ips-auto-update)# $s-auto-update/IOS_reqSeq-dw.xml
Router(config-ips-auto-update)#^Z
Router#
*May 4 2006 15:50:28 MST: IPS Auto Update: setting update timer for next update: 0 hrs 10
min
*May 4 2006 15:50:28 MST: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router#
```

```
Router# show ip ips auto-update

IPS Auto Update Configuration
    URL : tftp://192.168.0.2/jdoe/ips-auto-update/IOS_reqSeq-dw.xml
    Username : not configured
    Password : not configured
    Auto Update Intervals
      minutes (0-59) : 0
      hours (0-23) : 0-23
      days of month (1-31) : 1-31
      days of week: (0-6) : 1-5
```

Related Commands

Command	Description
ip ips auto-update	Enables automatic signature updates for Cisco IOS IPS.

show ip ips category

To display the Intrusion Prevention Detection (IPS) categories, use the **show ip ips category** command in user EXEC or privileged EXEC mode.

show ip ips category *category-name* [*subcategory-name*] [**config**]

Syntax Description

category-name	The configured IPS categories. Table 152 in the "Usage Guidelines" lists the *category-name* values.
subcategory-name	(Optional) The configured IPS subcategories. Table 152 in the "Usage Guidelines" lists the *subcategory-name* values.
config	Specifies the configuration values.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Use the **show ip ips category** command to display the IPS categories configured in the network.

Table 152 lists the values for the *category-name* and *subcategory-name* that can be configured for the **show ip ips category** command:

Table 152 Categories and Subcategories for the show ip ips category Command

Category Name	Description
adware/spyware	Displays information about the configured adware and spyware categories. The subcategory-name can be one of the following values: • **all-adware/spyware**—Advertising-supported software or spyware • **config**—Configuration values
attack	Displays information about the configured attack categories. The subcategory-name can be one of the following values: • **code_execution**—Code execution attack • **command_execution**—Command execution attack • **config**—Configuration values • **file_access**—File access • **general_attack**—General attack • **ids_evasion**—Intrusion Detection System (IDS) evasion • **informational**—Attack on the information resident in a network • **policy_violation**—Policy violation
ddos	Displays information about the configured Distributed Denial of Service attack categories. The subcategory-name can be one of the following values: • **all-ddos**—All Distributed Denial of Service attacks • **config**—Configuration values
dos	Displays information about the configured Denial of Service attack categories. The subcategory-name can be one of the following values: • **config**—Configuration values • **icmp_floods**—Internet Control Message Protocol flooding of the network • **tcp_floods**—Transmission Control Protocol flooding of the network • **udp_floods**—User Datagram Protocol flooding of the network
email	Displays the configured email clients. The subcategory-name can be one of the following values: • **config**—Configuration values • **imap**—Internet Message Access Protocol • **pop**—Post Office Protocol • **smtp**—Simple Mail Transfer Protocol

Table 152 Categories and Subcategories for the show ip ips category Command (continued)

Category Name	Description
instant_messaging	Displays the configured instant messaging clients. The subcategory-name can be one of the following values: • **aol**—America Online • **config**—Configuration values • **jabber**—Jabber instant messaging • **msn**—Microsoft Network • **sametime**—IBM Lotus Sametime Connect • **yahoo**—Yahoo messaging service
ios_ips	Displays signature information, such as the signatures that are disabled or marked for deletion. The subcategory-name can be one of the following values: • **advanced**—Advanced category • **basic**—Basic category • **config**—Configuration values • **default**—Default category
l2/l3/l4_protocol	Displays the list of configured Layer 2, Layer 3, and Layer 4 protocols. The subcategory-name can be one of the following values: • **arp**—Address Resolution Protocol • **config**—Configuration values • **general_protocol**—General protocol • **ip**—Internet Protocol. The subcategory-name can be one of the following values: – **config**—Configuration values – **general_ip**—General Internet Protocol – **icmp**—Internet Control Message Protocol – **ip_fragment**—IP Fragment – **ip_v6**—Internet Protocol Version 6 – **tcp**—Transmission Control Protocol – **udp**—User Datagram Protocol
network_services	Displays the configured routing protocols. The subcategory-name can be one of the following values: • **bgp**—Border Gateway Protocol • **config**—Configuration values • **dhcp**—Dynamic Host Configuration Protocol • **dns**—Domain Name Server • **finger**—Finger User Information Protocol

Table 152 Categories and Subcategories for the show ip ips category Command (continued)

Category Name	Description
os	Displays the configured operating system. The subcategory-name can be one of the following values: • **config**—Configuration values • **general_os**—General operating system • **ios**—Internetwork Operating System • **mac_os**—Mac operating system • **netware**—Netware operating system • **unix**—UNIX operating systems. The subcategory-name can be one of the following values: – **aix**—Advanced Interactive eXecutive operating system – **config**—Configuration values – **general-unix**—UNIX operating system – **hp-ux**—Hewlett-Packard UNIX operating system – **irix**—IRIX operating system – **linux**—Linux operating system – **solaris**—Solaris operating system • **windows**—Windows operating systems. The subcategory-name can be one of the following values: – **config**—Configuration values – **general_windows**—General Windows – **windows_nt/2k/xp**—Windows NT, Windows 2000, or Windows XP operating systems. You can specify the following keywords: **config**, **general_windows_nt/2k/xp**, and **winnt**.

Table 152 Categories and Subcategories for the show ip ips category Command (continued)

Category Name	Description
other_services	Displays the other protocols configured. The subcategory-name can be one of the following values: • **config**—Configuration values • **ftp**—File Transfer Protocol • **general_service**—General service • **http**—Hypertext Transfer Protocol • **https**—Hypertext Transfer Protocol Secure • **ident**—Ident protocol • **lpr**—Line Printer Daemon protocol • **msrpc**—Microsoft Remote Procedural Call • **netbios/smb**—Network Basic Input/Output System or Server Message Block • **nntp**—Network News Transfer Protocol • **ntp**—Network Time Protocol • **r-services**—R services • **rpc**—Remote Procedural Call • **snmp**—Simple Network Management Protocol • **socks**—SOCKS • **sql**—Structured Query Language • **ssh**—Secure Shell Remote Protocol • **telnet**—Telnet Remote Protocol • **tftp**—Trivial File Transport Protocol
p2p	Displays the configured peer-to-peer networks for file sharing. The subcategory-name can be one of the following values: • **bittorrent**—BitTorrent • **config**—Configuration values • **edonkey**—eDonkey • **kazaa**—Kazaa
reconnaissance	Displays the configured network reconnaissance categories. The subcategory-name can be one of the following values: • **config**—Configuration values • **icmp_host_sweeps**—Internet Control Message Protocol Host Sweeps • **tcp/udp_combo_sweeps**—Transmission Control Protocol or User Datagram Protocol Combo Sweeps • **tcp_ports_sweeps**—Transmission Control Protocol Port Sweeps • **udp_port_sweeps**—User Datagram Protocol Port Sweeps

Table 152 Categories and Subcategories for the show ip ips category Command (continued)

Category Name	Description
viruses/worms/trojans	Displays the viruses, worms, and trojans against which the network is configured. The subcategory-name can be one of the following values: • **all-viruses/worms/trojans**—All viruses, worms, and trojans that attack a network • **config**—Configuration values
web_server	Displays the configured Web servers. The subcategory-name can be one of the following values: • **apache**—Apache Web server • **config**—Configuration values • **internet_information_server_(iis)**—IIS Web server

Examples

The following examples display the output from variations of the **show ip ips category** command. The field names are self-explanatory.

```
Router# show ip ips category attack

Signatures in command_execution:
Signatures in general_attack:
Signatures in informational:
Signatures in file_access:
Signatures in code_execution:
Signatures in policy_violation:
Signatures in ids_evasion:

Router# show ip ips category instant_messaging

Signatures in yahoo:
Signatures in aol:
Signatures in msn:
Signatures in sametime:
Signatures in jabber:
```

Related Commands

Command	Description
ip ips	Applies an IPS rule to an interface.

show ip ips event-action-rules

To display event action rules information, use the **show ip ips event-action-rules** command in privileged EXEC mode.

show ip ips event-action-rules {**filters** | **overrides** | **target-value-rating** }

Syntax Description

filters	Displays the signature event action filters.
overrides	Displays the signature event action overrides.
target-value-rating	Displays the target value rating.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4 (11)T	This command was introduced.

Usage Guidelines

Event action rules are a group of settings you configure for the event action processing component of the sensor. These rules dictate the actions the sensor performs when an event occurs. Use the **show ip ips event-action-rules** command to display event action rules information, including default values that may not be displayed using the **show running-config** command.

Examples

The following example shows the global filter status for the event-action-rules. The output is self-explanatory.

```
Router# show ip ips event-action-rules filters
Filters

Global Filters Status: Enabled
```

The following example shows the global overrides status for the event-action-rules. The output is self-explanatory.

```
Router# show ip ips event-action-rules overrides
Overrides

Global Overrides Status: Enabled
Action to Add                    Enabled  Risk Rating
```

The following example shows the target-value-rating configuration status for the event-action-rules.The output is self-explanatory.

```
Router# show ip ips event-action-rules target-value-rating
No Target Value Ratings are configured
```

Related Commands

Command	Description
category	Displays category information.
configuration	Displays the IPS configuration information.
interfaces	Displays the IPS interfaces information.
ip ips all	Displays all IPS information.
ip ips auto-update	Enables automatic signature updates for Cisco IOS IPS.
name	Displays IPS name.
sessions	Displays IPS sessions.
signature-category	Displays signature category.
signatures	Displays IPS signatures.
statistics	Resets statistics on packets analyzed and alarms sent.

show ip ips signature-category

To display Cisco IOS Intrusion Prevention System (IPS) signature parameters by signature category, use the **show ip ips signature-category** command in privileged EXEC mode.

show ip ips signature-category [**config**]

Syntax Description

config	(Optional) Specifies configuration parameters for the signature categories.

Command Default

All the available signatures for the categories are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use the **show ip ips signature-category** command to verify the IPS signature parameters configured on the basis of a signature category.

Examples

The following is sample output from the **show ip ips signature-category** command:

```
Router# show ip ips signature-category

Signatures in basic:
Signatures in advanced:
Signatures in general_unix:
Signatures in general_linux:
Signatures in redhat:
Signatures in gentoo:
Signatures in mandrake:
Signatures in suse:
Signatures in solaris:
Signatures in hp-ux:
Signatures in aix:
Signatures in irix:
Signatures in general_windows:
Signatures in general_windows_nt/2k/xp:
Signatures in winnt:
Signatures in ios:
Signatures in general_os:
Signatures in netware:
Signatures in mac_os:
Signatures in command_execution:
Signatures in general_attack:
Signatures in informational:
Signatures in file_access:
```

The following example shows the **show ip ips signature-category** command output with the configured signature parameters:

```
Router# show ip ips signature-category config

    Category all:
        Retire: True
    Category IOSIPS 256mb:
        Retire: False
```

Related Commands

Command	Description
ip ips signature-category	Tunes IPS signature parameters per category.
show ip ips	Displays IPS configuration information.

show ip nhrp nhs

To display Next Hop Resolution Protocol (NHRP) next hop server (NHS) information, use the **show ip nhrp nhs** command in user EXEC or privileged EXEC mode.

show ip nhrp nhs [*interface-type interface-number*] [**detail** | **redundancy** [**cluster** *number* | **preempted** | **running** | **waiting**]

Syntax Description

interface-type	(Optional) Type of interface for which NHS information should be displayed. See Table 153 for types, number ranges, and descriptions.
interface-number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
detail	(Optional) Displays detailed NHS information.
redundancy	(Optional) Displays NHS recovery information.
cluster *number*	(Optional) Displays NHS recovery information based on the cluster value. The range is from 0 to 10.
preempted	(Optional) Displays NHSs that are declared as down and not actively probed.
running	(Optional) Displays NHSs that are responding or expecting replies.
waiting	(Optional) Displays NHSs that are waiting to be scheduled.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(2)T	This command was modified. The **redundancy**, **cluster** *number*, **preempted**, **running**, and **waiting** keywords and argument were added.

Usage Guidelines

Table 153 lists the valid types, number ranges, and descriptions for the optional *interface-number* argument.

Note The valid types can vary according to the platform and interfaces on the platform.

Table 153 Valid Types, Number Ranges, and Interface Descriptions

Valid Types	Number Ranges	Interface Descriptions
async	1	Async
atm	0 to 6	ATM
bvi	1 to 255	Bridge-Group Virtual Interface
cdma-ix	1	CDMA Ix
ctunnel	0 to 2147483647	C-Tunnel
dialer	0 to 20049	Dialer
ethernet	0 to 4294967295	Ethernet
fastethernet	0 to 6	Fast Ethernet IEEE 802.3
lex	0 to 2147483647	Lex
loopback	0 to 2147483647	Loopback
mfr	0 to 2147483647	Multilink Frame Relay bundle
multilink	0 to 2147483647	Multilink group
null	0	Null
port-channel	1 to 64	Port channel
tunnel	0 to 2147483647	Tunnel
vif	1	PGM multicast host
virtual-ppp	0 to 2147483647	Virtual PPP
virtual-template	1 to 1000	Virtual template
virtual-tokenring	0 to 2147483647	Virtual Token Ring
xtagatm	0 to 2147483647	Extended tag ATM

Examples

The following is sample output from the **show ip nhrp nhs detail** command:

```
Router# show ip nhrp nhs detail

Legend:
  E=Expecting replies
  R=Responding

Tunnel1:
  10.1.1.1           E  req-sent 128  req-failed 1  repl-recv 0

Pending Registration Requests:
Registration Request: Reqid 1, Ret 64  NHS 10.1.1.1
```

The following is sample output from the **show ip nhrp nhs** command:

```
Router# show ip nhrp nhs

Legend: E=Expecting replies, R=Responding, W=Waiting
Tunnel0:
192.0.2.1  W priority = 2 cluster = 0
192.0.2.2  RE priority = 0 cluster = 0
192.0.2.3  RE priority = 1 cluster = 0
```

The following is sample output from the **show ip nhrp nhs redundancy** command:

```
Router# show ip nhrp nhs redundancy

Legend: E=Expecting replies, R=Responding, W=Waiting
No.  Interface  Cluster  NHS          Priority  Cur-State  Cur-Queue  Prev-State Prev-Queue
1    Tunnel0    0        10.0.0.253   3         RE         Running    E          Running
2    Tunnel0    0        10.0.0.252   2         RE         Running    E          Running
3    Tunnel0    0        10.0.0.251   1         RE         Running    E          Running

No.  Interface  Cluster  Status   Max-Con Total-NHS Responding Expecting Waiting Fallback
1    Tunnel0    0        Enable   3       3         3          0         0       0
```

Table 154 describes the significant fields shown in the displays.

Table 154 show ip nhrp nhs Field Descriptions

Field	Description
Tunnel1	Interface through which the target network is reached.
priority	Priority value assigned to the NHS.
cluster	Group to which the NHS belong to.
W=Waiting	NHSs that are preempted and are not in the active probe list.
E=Expecting replies	NHSs that are active and expecting replies.
R=Responding	NHSs that are active and responding.

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
show ip nhrp	Displays NHRP mapping information.
show ip nhrp multicast	Displays NHRP multicast mapping information.
show ip nhrp summary	Displays NHRP mapping summary information.
show ip nhrp traffic	Displays NHRP traffic statistics.

show ip port-map

To display the port-to-application mapping (PAM) information, use the **show ip port-map** command in privileged EXEC mode.

show ip port-map [*appl-name* | **port** *port-num* [**detail**]]

Syntax Description

appl-name	(Optional) Specifies the name of the application to which to apply the port mapping.
port *port-num*	(Optional) Specifies the alternative port number that maps to the application.
detail	(Optional) Shows the port or application details.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(14)T	The **detail** keyword was added and command output was modified to display user-defined applications.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to display the port mapping information at the firewall, including the system-defined and user-defined information. Include the application name to display the list of entries by application. Include the port number to display the entries by port.

Examples

The following is sample output from the **show ip port-map** command, including system- and user-defined mapping information. Notice that multiple port numbers display in a series such as 554, 8554, or 1512...1525, or a range such as 55000 to 62000. When there are multiple ports, they all display if they can fit into the fixed-field width. If they cannot fit into the fixed-field width, they display with an ellipse, such as 1512...1525 shown below.

```
Router# show ip port-map

Default mapping:  snmp       udp port 161                    system defined
Host specific:    snmp       udp port 577         in list 55 user defined
Host specific:    snmp       udp port 55000-62000 in list 57 user defined
Default mapping:  echo       tcp port 7                      system defined
Default mapping:  echo       udp port 7                      system defined
Default mapping:  telnet     tcp port 23                     system defined
Default mapping:  wins       tcp port 1512...1525            system defined
Default mapping:  n2h2server tcp port 9285                   system defined
Default mapping:  n2h2server udp port 9285                   system defined
Default mapping:  nntp       tcp port 119                    system defined
```

```
Default mapping:  pptp       tcp port 1725                  system defined
Default mapping:  rtsp       tcp port 554,8554              system defined
Default mapping:  bootpc     udp port 68                    system defined
Default mapping:  gdoi       udp port 848                   system defined
Default mapping:  tacacs     udp port 49                    system defined
Default mapping:  gopher     tcp port 70                    system defined
Default mapping:  icabrowser udp port 1604                  system defined
```

The following sample output from the **show ip port-map snmp** command displays information about the SNMP application:

```
Router# show ip port-map snmp

Default mapping:  snmp    udp port 161                      system defined
Host specific:    snmp    udp port 577          in list 55  user defined
Host specific:    snmp    udp port 55000-62000  in list 57  user defined
```

The following sample output from the **show ip port-map snmp detail** command displays detailed information about the SNMP application:

```
Router# show ip port-map snmp detail

 IP port-map entry for application 'snmp':
     udp 161                   Simple Network Management Protoco system defined
     udp 577            list 55 User's SNMP Port                 user defined
     udp 55000-62000    list 57 User's Another SNMP Port         user defined
```

The following sample output from the **show ip port-map port 577** command displays information about port 577:

```
Router# show ip port-map port 577

Host specific:   snmp  udp port 577    in list 55   user defined
```

The following sample output from the **show ip port-map port 55800** command displays information about port 55800:

```
Router# show ip port-map port 55800

Host specific:   snmp   udp port 55800  in list 57   user defined
```

The following sample output from the **show ip-port-map port 577 detail** command displays detailed information about port 577:

```
Router# show ip port-map port 577 detail

 IP Port-map entry for port 577:
 snmp                udp list 55                           user defined
```

Related Commands

Command	Description
ip port-map	Establishes PAM entries.

show ip sdee

To display Security Device Event Exchange (SDEE) notification information, use the **show ip sdee** command in privileged EXEC mode.

show ip sdee {[**alerts**] [**all**] [**errors**] [**events**] [**configuration**] [**status**] [**subscriptions**]}

Syntax Description

alerts	Displays the Intrusion Detection System (IDS) alert buffer.
all	Displays all information available for IDS SDEE notifications.
errors	Displays IDS SDEE error messages.
events	Displays IDS SDEE events.
configuration	Displays SDEE configuration parameters.
status	Displays the status events that are currently in the buffer.
subscriptions	Displays IDS SDEE subscription information.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following is sample output from the **show ip sdee alerts** command. In this example, the alerts are numbered from 1 to 100 (because 100 events are currently in the event buffer). Following the alert number are 3 digits, which indicate whether the alert has been reported for the 3 possible subscriptions. In this example, these alerts have been reported for subscription number 1. The event ID is composed of the alert time and an increasing count, separated by a colon.

```
Router# show ip sdee alerts

Event storage:1000 events using 656000 bytes of memory
                                SDEE Alerts

SigID       SrcIP     DstIP       SrcPort  DstPort  Sev     Event ID        SigName
1:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211478597901  ICMP Echo Req
2:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211478887902  ICMP Echo Req
3:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211479247903  ICMP Echo Req
4:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211479457904  ICMP Echo Req
5:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211479487905  ICMP Echo Req
6:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211480077906  ICMP Echo Req
7:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211480407907  ICMP Echo Req
.....
.....
96:000 2004 10.0.0.2  10.0.0.1    8        0        2       10211750898596  ICMP Echo Req
97:000 2004 10.0.0.2  10.0.0.1    8        0        2       10211750898597  ICMP Echo Req
98:000 2004 10.0.0.2  10.0.0.1    8        0        2       10211750898598  ICMP Echo Req
99:000 2004 10.0.0.2  10.0.0.1    8        0        2       10211750908599  ICMP Echo Req
100:000 2004 10.0.0.2 10.0.0.1    8        0        2       10211750918600  ICMP Echo Req
```

The following is sample output is from the **show ip sdee subscriptions** command. In this example, SDEE is enabled, the maximum event buffer size has been set to 100, and the maximum number of subscriptions that can be open at the same time is 1.

```
Router# show ip sdee subscriptions

SDEE is enabled
Alert buffer size:100 alerts 65600 bytes
Maximum subscriptions:1

SDEE open subscriptions: 1
Subscription ID IDS1720:0:
Client address 10.0.0.2 port 1500
        Subscription opened at 13:21:30 MDT July 18 2003
        Total GET requests:0
        Max number of events:50
        Timeout:30
        Event Start Time:0
        Report alerts:true
        Alert severity level is INFORMATIONAL
        Report errors:false
        Report status:false
```

Table 155 describes the significant fields shown in the display.

Table 155 show ip sdee subscriptions Field Descriptions

Field	Description
Alert buffer size:100 alerts 65600 bytes	Maximum number of events that can be stored in the buffer. The maximum number of events to be stored refers to all types of events (alert, status, and error). (This value can be changed via the **ip sdee events** command.)
Maximum subscriptions:1	Maximum number of subscriptions that can be open at the same time. (This value can be changed via the **ip sdee subscriptions** command.)

The following is sample output from the **show ip sdee status** command. In this example, the buffer is set to store a maximum of 1000 events.

```
Router# show ip sdee status

Event storage:1000 events using 656000 bytes of memory

                  SDEE Status Messages
Time                            Message              Description
1:000 22:10:58 UTC Apr 18 2003  applicationStarted   STRING.UDP,0 ms
2:000 22:10:58 UTC Apr 18 2003  applicationStarted   STRING.TCP,0 ms
3:000 22:10:58 UTC Apr 18 2003  applicationStarted   OTHER,0 ms
4:000 22:10:58 UTC Apr 18 2003  applicationStarted   SERVICE.FTP,276 ms
5:000 22:11:07 UTC Apr 18 2003  applicationStarted   SERVICE.SMTP,8884 ms
6:000 22:11:07 UTC Apr 18 2003  applicationStarted   SERVICE.RPC,72 ms
7:000 22:11:07 UTC Apr 18 2003  applicationStarted   SERVICE.DNS,132 ms
8:000 22:11:15 UTC Apr 18 2003  applicationStarted   SERVICE.HTTP,7632 ms
9:000 22:11:15 UTC Apr 18 2003  applicationStarted   ATOMIC.TCP,24 ms
10:000 22:11:15 UTC Apr 18 2003  applicationStarted  ATOMIC.UDP,12 ms
11:000 22:11:15 UTC Apr 18 2003  applicationStarted  ATOMIC.ICMP,12 ms
12:000 22:11:15 UTC Apr 18 2003  applicationStarted  ATOMIC.IPOPTIONS,8 ms
13:000 22:11:15 UTC Apr 18 2003  applicationStarted  ATOMIC.L3.IP,8 ms
```

Related Commands

Command	Description
ip ips notify	Specifies the method of event notification.
id sdee events	Sets the maximum number of SDEE events that can be stored in the event buffer.
ip sdee subscriptions	Sets the maximum number of SDEE subscriptions that can be open simultaneously.

show ip ips sig-clidelta

To display the signature parameter tunings configured using the CLI that are stored in the iosips-sig-clidelta.xmz signature file, use the **show ip ips sig-clidelta** command in privileged EXEC mode.

show ip ips sig-clidelta

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **show ip ips sig-clidelta** command displays the tunings configured from the CLI that are stored in the iosips-sig-clidelta.xmz signature file.

Examples

The following is sample output from the **show ip ips sig-clidelta** command. The field descriptions are self-explanatory.

```
Router# show ip ips sig-clidelta

En  - possible values are Y, Y*, N, or N*
      Y:  signature is enabled
      N:  enabled=false in the signature definition file
      *:  retired=true in the signature definition file
Cmp - possible values are Y, Ni, Nr, Nf, or No
      Y:  signature is compiled
      Ni: signature not compiled due to invalid or missing parameters
      Nr: signature not compiled because it is retired
      Nf: signature compile failed
      No: signature is obsoleted
      Nd: signature is disallowed
Action=(A)lert, (D)eny, (R)eset, Deny-(H)ost, Deny-(F)low
Trait=alert-traits             EC=event-count          AI=alert-interval
GST=global-summary-threshold   SI=summary-interval     SM=summary-mode
SW=swap-attacker-victim        SFR=sig-fidelity-rating Rel=release

 SigID:SubID En  Cmp   Action Sev   Trait   EC   AI   GST   SI  SM SW SFR Rel
 ----------- --  ----  ------ ---   -----  ---- ---- -----  --- -- -- --- ---
  5733:0     N   Y     A     HIGH     0     1    0      0    0  FA  N 85  S266
```

Related Commands

Command	Description
ip ips enable-clidelta	Enables the signature tuning settings in the clidelta.xmz file on the router to take precedence over the signature settings in the iosips-sig-delta.xmz file.

show ip source-track

To display traffic flow statistics for tracked IP host addresses, use the **show ip source-track** command in privileged EXEC mode.

show ip source-track [*ip-address*] [**summary** | **cache**]

Syntax Description

ip-address	(Optional) Displays the IP address of the tracked host for which traffic flow information is displayed.
summary	(Optional) Displays a summary of traffic flow information that is collected for a specified host address (via the *ip-address* argument) or for all configured hosts.
cache	(Optional) Displays detailed packet and flow information that is collected on line cards and port adapters for all tracked IP addresses or for specified IP address (not displayed in the a distributed platform such as the gigabit route processor (GRP) or route switch processor (RSP)).

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(21)S	This command was introduced.
12.0(22)S	This command was implemented on the Cisco 7500 series routers.
12.0(26)S	This command was implemented on Cisco 12000 series ISE line cards.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example, which is sample output from the **show ip source-track summary** command, shows how to verify that IP source tracking is enabled for one or more hosts:

```
Router# show ip source-track summary

Address          Bytes    Pkts    Bytes/s   Pkts/s
10.0.0.1          119G   1194M    443535      4432
192.168.1.1       119G   1194M    443535      4432
192.168.42.42     119G   1194M    443535      4432
```

The following example, which is sample output from the **show ip source-track summary** command, shows how to verify that no traffic has yet to be received for the destination hosts that are being tracked:

```
Router# show ip source-track summary

Address        Bytes   Pkts   Bytes/s   Pkts/s
10.0.0.1           0      0         0        0
```

```
192.168.1.1         0       0          0         0
192.168.42.42       0       0          0         0
```

The following example, which is sample output from the **show ip source-track** command, shows that IP source tracking is processing packets to the hosts and exporting statistics from the line card or port adapter to the route processor:

```
Router# show ip source-track

Address          SrcIF    Bytes   Pkts   Bytes/s   Pkts/s
10.0.0.1         PO0/0    119G   1194M    513009     5127
192.168.1.1      PO0/0    119G   1194M    513009     5127
192.168.42.42    PO0/0    119G   1194M    513009     5127
```

Related Commands

Command	Description
ip source-track	Enables IP source tracking for a specified host.
ip source-track address-limit	Configures the maximum number of destination hosts that can be simultaneously tracked at any given moment.
ip source-track syslog-interval	Sets the time interval (in minutes) in which syslog messages are generated if IP source tracking is enabled on a device.

show ip source-track export flows

To display the last ten packet flows that were exported from the line card to the route processor, use the **show ip source-track export flows** command in privileged EXEC mode.

show ip source-track export flows

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(21)S	This command was introduced.
12.0(22)S	This command was implemented on the Cisco 7500 series routers.
12.0(26)S	This command was implemented on Cisco 12000 series ISE line cards.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show ip source-track export flows** command can be issued only on distributed platforms such as the GRP and the RSP.

Examples

The following example displays the packet flow information that is exported from line cards and port adapters to the gigabit route processor (GRP) and the route switch processor (RSP):

```
Router# show ip source-track export flows

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
PO0/0         10.1.1.0        Null          10.1.1.1        06 0000 0000    88K
PO0/0         10.1.1.0        Null          10.1.1.3        06 0000 0000    88K
PO0/0         10.1.1.0        Null          10.1.1.2        06 0000 0000    88K
```

Related Commands

Command	Description
ip source-track	Enables IP source tracking for a specified host.
ip source-track export-interval	Sets the time interval (in seconds) in which IP source tracking statistics are exported from the line card to the RP.

show ip ssh

To display the version and configuration data for Secure Shell (SSH), use the **show ip ssh** command in privileged EXEC mode.

show ip ssh

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1 T.
12.1(5)T	This command was modified to display the SSH status—enabled or disabled.
12.2(17a)SX	This command was integrated into Cisco IOS Release 12.2(17a)SX.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

Use the **show ip ssh** command to view the status of configured options such as retries and timeouts. This command allows you to see if SSH is enabled or disabled.

Examples

The following is sample output from the **show ip ssh** command when SSH has been enabled:

```
Router# show ip ssh

SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
```

The following is sample output from the **show ip ssh** command when SSH has been disabled:

```
Router# show ip ssh

%SSH has not been enabled
```

Related Commands

Command	Description
show ssh	Displays the status of SSH server connections.

show ip traffic-export

To display information related to router IP traffic export (RITE), use the **show ip traffic-export** command in privileged EXEC mode.

show ip traffic-export [**interface** *interface-name* | **profile** *profile-name*]

Syntax Description

interface *interface-name*	(Optional) Only data associated with the monitored ingress interface is shown.
profile *profile-name*	(Optional) Only flow statistics, such as exported packets and number of bytes, are shown.

Defaults

If this command is enabled, all data (both interface- and profile-related data) is shown.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following sample output from the **show ip traffic-export** command is for the profile "one." This example is for a single configured interface. If multiple interfaces are configured, the information shown below is displayed for each interface.

```
Router# show ip traffic-export

Router IP Traffic Export Parameters
Monitored Interface             FastEthernet0/0
        Export Interface                FastEthernet0/1
        Destination MAC address 0030.7131.abfc
        bi-directional traffic export is off
Input IP Traffic Export Information     Packets/Bytes Exported    0/0
        Packets Dropped           0
        Sampling Rate             one-in-every 1 packets
        No Access List configured
        Profile one is Active
```

Table 156 describes the significant fields shown in the display.

Table 156 show ip traffic-export Field Descriptions

Field	Description
Monitored Interface	Interface in which the profile was applied. (This interface is specified via the **ip traffic-export apply profile** command.)
Export Interface	Interface in which the profile exports all captured IP traffic. (This interface is specified via the **ip traffic-export profile** command.)
Destination MAC address	Ethernet address of the destination host, which is specified via the **mac-address** command.
bi-directional traffic export is	Incoming and outgoing IP traffic is exported on the monitored interface (via the **bidirectional** command). By default, only incoming traffic is exported.
Input IP Traffic Export Information Packets Dropped Sampling Rate No Access List Configured Profile one is Active	Incoming IP traffic information. The sampling rate and ACL can be defined via the **incoming** command. If the profile is incomplete, the profile will be listed as inactive.

Related Commands

Command	Description
bidirectional	Enables incoming and outgoing IP traffic to be exported across a monitored interface.
ip traffic-export apply profile	Applies an IP traffic export profile to a specific interface.
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.
incoming	Configures filtering for incoming export traffic.
outgoing	Configures filtering for outgoing export traffic.

show ip trigger-authentication

To display the list of remote hosts for which automated double authentication has been attempted, use the **show ip trigger-authentication** command in privileged EXEC mode.

show ip trigger-authentication

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Whenever a remote user needs to be user-authenticated in the second stage of automated double authentication, the local device sends a User Datagram Protocol (UDP) packet to the remote user's host. When the UDP packet is sent, the user's host IP address is added to a table. If additional UDP packets are sent to the same remote host, a new table entry is not created; instead, the existing entry is updated with a new time stamp. This remote host table contains a cumulative list of host entries; entries are deleted after a timeout period or after you manually clear the table using the **clear ip trigger-authentication** command. You can change the timeout period with the **ip trigger-authentication** (global) command.

Use this command to view the list of remote hosts for which automated double authentication has been attempted.

Examples

The following example shows output from the **show ip trigger-authentication** command:

```
Router# show ip trigger-authentication

Trigger-authentication Host Table:
Remote Host          Time Stamp
209.165.200.230       2940514234
```

This output shows that automated double authentication was attempted for a remote user; the remote user's host has the IP address 209.165.200.230. The attempt to automatically double authenticate occurred when the local host (myfirewall) sent the remote host (209.165.200.230) a packet to UDP port 7500. (The default port was not changed in this example.)

Related Commands

Command	Description
clear ip trigger-authentication	Clears the list of remote hosts for which automated double authentication has been attempted.

show ip trm config

To display the configuration information for the Trend Router Provisioning Server (TRPS), use the **show ip trm config** command in privileged EXEC mode.

show ip trm config

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **show ip trm config** command to display information about the TRPS. The output shows both the current configuration and the default configuration.

Examples

The following shows sample output from the **show ip trm config** command when the router is registered with the TRPS named trps.example.com:

```
Router# show ip trm config

 Server: trps.example.com
   HTTPS Port: 443
   HTTP  Port: 80
       Status: Active

 Server: trps.trendmicro.com ( Default )
   HTTPS Port: 443
   HTTP  Port: 80
       Status: Standby
```

Table 157 describes the significant fields shown in the display.

Table 157 show ip trm config Field Descriptions

Field	Description
Server	The name of the TRPS.
HTTPS Port	The port on which the TRPS listens for secure HTTP requests.
HTTP Port	The port on which the TRPS listens for HTTP requests.
Status	The status of the named TRPS—either Active or Standby.

Related Commands

Command	Description
show ip trm subscription status	Displays the status of the subscription with Trend Micro.

show ip trm subscription status

To display information about the status of the Trend Micro subscription, use the **show ip trm subscription status** command in privileged EXEC mode.

show ip trm subscription status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **show ip trm subscription status** command to display the status of the Trend Micro subscription. If the router is registered with the Trend Router Provisioning Server (TRPS), the router displays the subscription status information. If the router is not registered with the TRPS, a message indicating that the router is not registered is displayed.

Examples

The following shows sample output from **show ip trm subscription status** command when the router is registered with the TRPS:

```
Router# show ip trm subscription status

Package Name:Security & Productivity
 ------------------------------------------------
               Status:     Active
   Status Update Time:      08:55:07 MDT Thu Apr 3 2008
      Expiration-Date:      Tue Jul 21 10:12:59 2020

      Last Req Status:      Processed response successfully
   Last Req Sent Time:      08:55:07 MDT Thu Apr 3 2008
```

Table 157 describes the significant fields shown in the display.

Table 158 show ip trm subscription status Field Descriptions

Field	Description
Status	Displays the status of the Trend Micro subscription.
Status Update Time	Displays the time and date that status of the Trend Micro subscription was last updated.
Expiration Date	Displays the date and time that the Trend Micro subscription expires.

Table 158 show ip trm subscription status Field Descriptions (continued)

Field	Description
Last Req Status	Displays the status of the most recent request.
Last Req Sent Time	Displays the time and date of the most recent lookup request to the TRPS.

Related Commands

Command	Description
show ip trm config	Displays information about the TRPS.

show ip urlfilter

To display Cisco IOS URL filtering information, use the **show ip urlfilter** command in privileged EXEC mode.

show ip urlfilter {**mib statistics** {**global** | **server** {**address** *ip-address* [**port** *port-number*] | **all**}} | **statistics** [**vrf** *vrf-name*]}

Syntax Description

mib	Displays the firewall MIB-specific URL filtering content.
statistics	Displays URL filtering statistics for the specified parameters.
global	Displays global URL filtering statistics.
server	Displays statistics for the specified server.
address *ip-address*	Specifies the IP address for the URL filtering server.
port *port-number*	(Optional) Displays statistics for the server specified using the service port.
all	Displays statistics for all configured servers.
vrf *vrf-name*	(Optional) Displays the information only for the specified virtual routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	The **vrf** keyword and *vrf-name* argument were added.
12.4(6)T	The following keywords and arguments were added: **all**, **address**, **global**, *ip-address*, **mib**, **port**, *port-number*, **server**.

Usage Guidelines

This command shows information such as the number of requests that are sent to the vendor server (Websense or N2H2), the number of responses received from the vendor server, the number of pending requests in the system, the number of failed requests, and the number of blocked URLs.

Examples

The following is sample output from the **show ip urlfilter statistics** command:

```
Router# show ip urlfilter statistics

URL filtering statistics
================
Current requests count:25
Current packet buffer count(in use):40
Current cache entry count:3100

Maxever request count:526
```

```
Maxever packet buffer count:120
Maxever cache entry count:5000

Total requests sent to URL Filter Server: 44765
Total responses received from URL Filter Server: 44550
Total requests allowed: 44320
Total requests blocked: 224
```

Table 159 describes the significant fields shown in the display.

Table 159 show ip urlfilter statistics Field Descriptions

Field	Description
Current requests count	Number of requests sent to the vendor server.
Current packet buffer count (in use)	Number of HTTP responses in the packet buffer of the firewall. This value can be specified via the ip urlfilter **max-resp-pak** command.
Current cache entry count	Number of destination IP addresses cached into the cache table. This value can be specified via the **ip urlfilter cache** command.
Maxever request count	Maximum number of requests that have been sent to the vendor server since power up. This value can be specified via the **ip urlfilter max-request** command.
Maxever packet buffer count	Maximum number of HTTP responses stored in the packet buffer of the firewall since power up. This value can be specified via the ip urlfilter **max-resp-pak** command.
Maxever cache entry count	Maximum number of destination IP addresses cached into the cache table since power up. This value can be specified via the **ip urlfilter cache** command.

The following is sample output when MIBs are enabled to track URL filtering statistics across the entire device (global). The output fields are self-explanatory.

```
Router# show ip urlfilter mib statistics global

URL Filtering Group Summary Statistics
------------------------------------------------------
URL Filtering Enabled
Requests Processed 260
Requests Processed 1-minute Rate 240
Requests Processed 5-minute Rate 215
Requests Allowed 230
Requests Denied 30
Requests Denied 1-minute Rate 15
Requests Denied 5-minute Rate 0
Requests Cache Allowed 5
Requests Cache Denied 5
Allow Mode Requests Allowed 15
Allow Mode Requests Denied 15
Requests Resource Dropped 0
Requests Resource Dropped 1-minute Rate 0
Requests Resource Dropped 5-minute Rate 0
Server Timeouts 0
Server Retries 0
Late Server Responses 0
Access Responses Resource Dropped 0
```

The following sample output when MIBs are enabled to track URL filtering statistics across the server with IP address 209.165.201.30. The output fields are self-explanatory.

```
Router# show ip urlfilter mib statistics server address 209.165.201.30

URL Filtering Server Statistics
-------------------------------------------------------
URL Server Host Name 209.165.201.30
Server Address 209.165.201.30
Server Port 15868
Server Vendor Websense
Server Status Online
Requests Processed 4
Requests Allowed 1
Requests Denied 3
Server Timeouts 0
Server Retries 9
Responses Received 1
Late Server Responses 12
1 Minute Average Response Time 0
5 Minute Average Response Time 0
```

Related Commands

Command	Description
ip urlfilter cache	Configures cache parameters.
ip urlfilter max-request	Sets the maximum number of outstanding requests that can exist at any given time.
ip urlfilter max-resp-pak	Configures the maximum number of HTTP responses that the firewall can keep in its packet buffer.

show ip urlfilter cache

To display the maximum number of entries that can be cached into the cache table and the number of entries and the destination IP addresses that are cached into the cache table, use the **show ip urlfilter cache** command in privileged EXEC mode.

show ip urlfilter cache [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the information only for the specified Virtual Routing and Forwarding (VRF) interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example is sample output from the **show ip urlfilter cache** command:

```
Router# show ip urlfilter cache

Maximum number of entries allowed: 5000
Number of entries cached: 5
IP addresses cached ....
 10.64.128.54
 172.28.139.21
 10.76.82.25
 192.168.0.1
 10.0.1.2
```

Table 160 describes the significant fields shown in the display.

Table 160 show ip urlfilter cache Field Descriptions

Field	Description
Maximum number of entries allowed	Maximum number of destination IP addresses that can be cached into the cache table. This parameter can be configured using the **ip url filter cache** command. (The default is 5000.)

Table 160 show ip urlfilter cache Field Descriptions

Field	Description
Number of entries cached	Number of entries that have already been cached into the cache table.
IP addresses cached	IP addresses that have already been cached into the cache table.

Related Commands

Command	Description
clear ip urlfilter cache	Clears the cache table.
ip urlfilter cache	Configures cache parameters.

show ip urlfilter config

To display the size of the cache, the maximum number of outstanding requests, the allow mode state, and the list of configured vendor servers, use the **show ip urlfilter config** command in EXEC mode.

show ip urlfilter config [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the information only for the specified Virtual Routing and Forwarding (VRF) interface.

Command Modes

EXEC

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	The **vrf** *vrf-name* keyword/argument pair was added.

Examples

The following example is sample output from the **show ip urlfilter config** command:

```
Router# show ip urlfilter config

URL filter is ENABLED

Primary Websense server configurations
==========================
Websense server IP address: 10.0.0.3
Websense server port: 15868
Websense retransmit time out: 5 (seconds)
Websense number of retransmit:2

Secondary Websense server configurations:
=============================
None.

Other configurations
===============
Allow mode: OFF
System Alert: ON
Log message on the router: OFF
Log message on URL filter server:ON
Maximum number of cache entries :5000
Cache timeout :12 (hours)
Maximum number of packet buffers:200
Maximum outstanding requests:1000
```

Related Commands

Command	Description
ip urlfilter allowmode	Turns on the default mode (allow mode) of the filtering algorithm.
ip urlfilter cache	Configures cache parameters.
ip urlfilter max-request	Sets the maximum number of outstanding requests that can exist at any given time.
ip urlfilter server vendor	Configures a vendor server for URL filtering.

show ip virtual-reassembly

To display the configuration and statistical information of the virtual fragment reassembly (VFR) on a given interface, use the **show ip virtual-reassembly** command in privileged EXEC mode.

show ip virtual-reassembly [**interface** *type*]

Syntax Description

interface *type*	(Optional) VFR information is shown only for the specified interface. If an interface is not specified, VFR information for all configured interfaces is shown.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following example is sample output from the **show ip virtual-reassembly** command:

```
Router# show ip virtual-reassembly interface ethernet1/1

Ethernet1/1:
Virtual Fragment Reassembly (VFR) is ENABLED...
Concurrent reassemblies (max-reassemblies):64
Fragments per reassembly (max-fragments):16
Reassembly timeout (timeout):3 seconds
Drop fragments:OFF

Current reassembly count:12
Current fragment count:48
Total reassembly count:6950
Total reassembly failures:9
```

Table 161 describes the significant fields shown in the display.

Table 161 show ip virtual-reassembly Field Descriptions

Field	Description
Concurrent reassemblies (max-reassemblies):64	Maximum number of IP datagrams that can be reassembled at any given time. Value can be specified via the **max-reassemblies** *number* option from the **ip virtual-reassembly** command.
Fragments per reassembly (max-fragments):16	Maximum number of fragments that are allowed per IP datagram (fragment set). Value can be specified via the **max-fragments** *number* option from the **ip virtual-reassembly** command.

Table 161 show ip virtual-reassembly Field Descriptions (continued)

Field	Description
Reassembly timeout (timeout):3 seconds	Timeout value for an IP datagram that is being reassembled. Value can be specified via the **timeout** *seconds* option from the **ip virtual-reassembly** command.
Drop fragments:OFF	Specifies whether the VFR should drop all fragments that arrive on the configured interface. Function can be turned on or off via the **drop-fragments** keyword from the **ip virtual-reassembly** command.
Current reassembly count	Number of IP datagrams that are currently being reassembled
Current fragment count	Number of fragments that have been buffered by VFR for reassembly
Total reassembly count	Total number of datagrams that have been reassembled since the last system reboot.
Total reassembly failures	Total number of reassembly failures since the last system reboot.

Related Commands

Command	Description
ip virtual-reassembly	Enables VFR on an interface.

show kerberos creds

To display the contents of your credentials cache, use the **show kerberos creds** command in privileged EXEC mode.

show kerberos creds

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show kerberos creds** command is equivalent to the UNIX klist command.

When users authenticate themselves with Kerberos, they are issued an authentication ticket called a *credential*. The credential is stored in a credential cache.

Examples

The following example displays entries in the credentials cache:

```
Router > show kerberos creds

 Default Principal: user@example.com
 Valid Starting          Expires                 Service Principal
 18-Dec-1995 16:21:07    19-Dec-1995 00:22:24    krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

The following example returns output that acknowledges that credentials do *not* exist in the credentials cache:

```
Router > show kerberos creds

 No Kerberos credentials
```

Related Commands

Command	Description
clear kerberos creds	Deletes the contents of the credentials cache.

show ldap attributes

To display attributes of the Lightweight Directory Access Protocol (LDAP) server, use the **show ldap attributes** command in user EXEC or privileged EXEC mode.

show ldap attributes

Syntax Description

This command has no arguments and keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

Use the **show ldap attributes** command to display the default mapping of LDAP attributes to AAA attributes. It displays the dynamic attribute map that is configured on the router.

Examples

The following is sample output from the **show ldap server** command:

```
Router# show ldap attributes

LDAP Attribute                    Format      AAA Attribute
==============                    ======      =============
airespaceBwDataBurstContract     Ulong       bsn-data-bandwidth-burst-contr
userPassword                     String      password
airespaceBwRealBurstContract     Ulong       bsn-realtime-bandwidth-burst-c
employeeType                     String      employee-type
airespaceServiceType             Ulong       service-type
airespaceACLName                 String      bsn-acl-name
priv-lvl                         Ulong       priv-lvl
memberOf                         String DN   supplicant-group
cn                               String      username
airespaceDSCP                    Ulong       bsn-dscp
policyTag                        String      tag-name
airespaceQOSLevel                Ulong       bsn-qos-level
airespace8021PType               Ulong       bsn-8021p-type
airespaceBwRealAveContract       Ulong       bsn-realtime-bandwidth-average
airespaceVlanInterfaceName       String      bsn-vlan-interface-name
airespaceVapId                   Ulong       bsn-wlan-id
airespaceBwDataAveContract       Ulong       bsn-data-bandwidth-average-con
sAMAccountName                   String      sam-account-name
meetingContactInfo               String      contact-info
telephoneNumber                  String      telephone-number

Map: att_map_1
department                       String DN   element-req-qos
```

Table 162 describes the significant fields shown in the display.

Table 162 show ldap attributes Descriptions

Field	Description
LDAP Attribute	LDAP distinguished name attribute (or attributes).
Format	Format conversion of the attribute.
AAA Attribute	Authentication, Authorization, and Accounting (AAA) distinguished name attribute (or attributes).

Related Commands

Command	Description
attribute-map	Attaches an attribute map to a particular LDAP server.
ldap attribute-map	Configures a dynamic LDAP attribute map.
map-type	Defines the mapping of an attribute in the LDAP server.
show ldap server	Displays properties of the LDAP server.

show ldap server

To display properties of the Lightweight Directory Access Protocol (LDAP) server, use the **show ldap server** command in user EXEC or privileged EXEC mode.

show ldap server {**name** | **all**}

Syntax Description

name	Displays properties for the LDAP server that has been configured.
all	Displays properties for all LDAP servers.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Examples

The following is sample output from the **show ldap server** command:

```
Router# show ldap server ldap-srv1

Server Information for ldap-srv1
================================
Server name :ls1
Server IP :10.64.67.106
Server listening Port :389
Connection status :UP
Root Bind status :Anonymous Bind Done
Server mode :Non-Secure
Cipher Suite :0x00
Authentication Seq :Search first. Then Bind/Compare password next
Authentication Procedure :Bind with user password
Base-Dn :dc=my-domain,dc=com
User Attribute :cn
Password Attribute :userPassword
Timeout retransmit :30
```

Table 163 describes the significant fields shown in the display.

Table 163 show ldap server Field Descriptions

Field	Description
Server name	LDAP server name.
Server IP	IP address of the LDAP server.
Server listening Port	The transport layer port server is listening on.
Connection status	Connection status of the LDAP server.
Root Bind status	Bind status in the LDAP server.

Table 163 show ldap server Field Descriptions (continued)

Field	Description
Server mode	Security mode.
Cipher Suite	Cryptographic algorithms used in the connection.
Authentication Seq	LDAP authentication sequence.
Authentication Procedure	Authentication method.
Base-Dn	Distinguished name of the search base.
User Attribute	Distinguished user name attribute (or attributes) that uniquely identifies an entry on the LDAP server.
Password Attribute	Distinguished password name attribute (or attributes) that uniquely identifies an entry on the LDAP server.
Timeout retransmit	Response timeout. Default timeout value is 30 seconds.

Related Commands

Command	Description
show ldap attribute	Displays information about default LDAP attribute mapping.

show logging ip access-list

To display information about the logging IP access list, use the **show logging ip access-list** command in privileged EXEC mode.

show logging ip access-list {**cache** | **config**}

Syntax Description

cache	Displays information about all the entries in the Optimized ACL Logging (OAL) cache.
config	Displays information about the logging IP access-list configuration.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXE	This command was changed to include the **config** keyword on the Supervisor Engine 720 only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720 only.

OAL is supported on IPv4 unicast traffic only.

Examples

This example shows how to display all the entries in the OAL cache:

```
Router# show logging ip access-list cache

Matched flows:
id prot src_ip dst_ip sport dport status count
total lastlog
-------------------------------------------------------------------------------------
1 17 10.2.1.82 10.2.12.2 111 63 Permit 0
3906 2d02h
2 17 10.2.1.82 10.2.12.2 1135 63 Permit 0
3906 2d02h
3 17 10.2.1.82 10.2.12.2 2159 63 Permit 0
3906 2d02h
4 17 10.2.1.82 10.2.12.2 3183 63 Permit 0
3906 2d02h
5 17 10.2.1.82 10.2.12.2 4207 63 Permit 0
3906 2d02h
6 17 10.2.1.82 10.2.12.2 5231 63 Deny 0
3906 2d02h
```

```
7 17 10.2.1.82 10.2.12.2 6255 63 Deny 0
3906 2d02h
8 17 10.2.1.82 10.2.12.2 7279 63 Permit 0
3906 2d02h
9 17 10.2.1.82 10.2.12.2 8303 63 Permit 0
3906 2d02h
10 17 10.2.1.82 10.2.12.2 9327 63 Permit 0
3905 2d02h
11 17 10.2.1.82 10.2.12.2 10351 63 Permit 0
3905 2d02h
12 17 10.2.1.82 10.2.12.2 11375 63 Permit 0
3905 2d02h
13 17 10.2.1.82 10.2.12.2 12399 63 Deny 0
3905 2d02h
14 17 10.2.1.82 10.2.12.2 13423 63 Permit 0
3905 2d02h
15 17 10.2.1.82 10.2.12.2 14447 63 Deny 0
3905 2d02h
16 17 10.2.1.82 10.2.12.2 15471 63 Permit 0
3905 2d02h
17 17 10.2.1.82 10.2.12.2 16495 63 Permit 0
3905 2d02h
18 17 10.2.1.82 10.2.12.2 17519 63 Permit 0
3905 2d02h
19 17 10.2.1.82 10.2.12.2 18543 63 Permit 0
3905 2d02h
20 17 10.2.1.82 10.2.12.2 19567 63 Permit 0
3905 2d02h

Number of entries: 20
Number of messages logged: 112
Number of packets logged: 11200
Number of packets received for logging: 11200
```

This example shows how to display information about the logging IP access-list configuration:

```
Router# show logging ip access-list config

Logging ip access-list configuration
 Maximum number of cached entries: 8192
 Logging rate limiter: 0
 Log-update interval: 300
 Log-update threshold: 0
 Configured on input direction:
        Vlan2
        Vlan1
 Configured on output direction:
        Vlan2
```

Related Commands

Command	Description
clear logging ip access-list cache	Clears all the entries from the OAL cache and sends them to the syslog.
logging ip access-list cache (global configuration)	Configures the OAL parameters.
logging ip access-list cache (interface configuration)	Enables an OAL-logging cache on an interface that is based on direction.

show login

To display login parameters, use the **show login** command in privileged EXEC mode.

show login [**failures**]

Syntax Description

failures	(Optional) Displays information related only to failed login attempts.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **show login** command allows users to verify the applied login configuration and present login status on your router.

Examples

The following sample output from the **show login** command verifies that no login parameters have been specified:

```
Router# show login

No login delay has been applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps

Router NOT enabled to watch for login Attacks
```

The following sample output from the **show login** command verifies that the **login block-for** command is issued. In this example, the command is configured to block login hosts for 100 seconds if 16 or more login requests fail within 100 seconds; 5 login requests have already failed.

```
Router# show login

A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.

Router enabled to watch for login Attacks.
If more than 15 login failures occur in 100 seconds or less, logins will be disabled for
100 seconds.
```

```
Router presently in Watch-Mode, will remain in Watch-Mode for 95 seconds.
Present login failure count 5.
```

The following sample output from the **show login** command verifies that the router is in quiet mode. In this example, the **login block-for** command was configured to block login hosts for 100 seconds if 3 or more login requests fail within 100 seconds.

```
Router# show login

A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.

Router enabled to watch for login Attacks.
If more than 2 login failures occur in 100 seconds or less, logins will be disabled for
100 seconds.

Router presently in Quiet-Mode, will remain in Quiet-Mode for 93 seconds.
Denying logins from all sources.
```

Table 164 describes the significant fields shown in the proceeding displays.

Table 164 show login Field Descriptions

Field	Description
A default login delay of 1 seconds is applied.	A delay of 1 second is enforced when the **login block-for** command is issued. To specify a different delay value, use the **login delay** command.
No Quiet-Mode access list has been configured.	No access control lists (ACLs) are exempt from the quiet period. To specify an ACL, use the **login quiet-mode access-class** command.
All successful or failed login is logged and generate SNMP traps.	Logging messages and Simple Network Management Protocol (SNMP) traps are configured to be generated upon successful or failed login attempts. To change this setting, use the **login on-success** or **login on-failure** command.
Router enabled to watch for login Attacks.	The Cisco IOS device has been configured with at least the **login block-for** command, which enables default login functionality. **Note** If no login parameters are specified, the following description appears: "Router NOT enabled to watch for login Attacks."
If more than 2 login failures occur in 100 seconds or less, logins will be disabled for 100 seconds.	Parameters of the **login block-for** *seconds* **attempts** *tries* **within** *seconds* command.

Table 164 show login Field Descriptions (continued)

Field	Description
Router presently in Quiet-Mode, will remain in Quiet-Mode for 93 seconds.	The router has switched to quiet mode. **Note** If the router is not in quiet mode, the following description appears: "Router presently in Watch-Mode, will remain in Watch-Mode for 95 seconds."
Denying logins from all sources.	The router is in quiet mode and no ACLs are defined, so the router is denying all login requests. **Note** If the router is not in quiet mode, the following description, which allows the user to keep track of the current failed login attempts, appears: "Present login failure count 5."

show login failure Sample Outputs

The following sample output from **show login failures** command shows all failed login attempts on the router:

```
Router# show login failures

Information about login failure's with the device

Username      Source IPAddr  lPort Count  TimeStamp
try1          10.1.1.1        23    1     21:52:49 UTC Sun Mar 9 2003
try2          10.1.1.2        23    1     21:52:52 UTC Sun Mar 9 2003
```

The following sample output from **show login failures** command verifies that no information is presently logged:

```
Router# show login failures

*** No logged failed login attempts with the device.***
```

Related Commands

Command	Description
login block-for	Configures your Cisco IOS device for login parameters that help provide DoS detection.
login delay	Configures a uniform delay between successive login attempts.
login on-failure	Generates system logging messages for every login attempts.
login on-success	Generates system logging messages for successful login attempts.
login quiet-mode access-class	Specifies an ACL that is to be applied to the router when it switches to quiet mode.

show mab

To display MAC Authentication Bypass (MAB) information, use the **show mab** command in privileged EXEC mode.

show mab {**all** | **interface** *type number*} [**detail**]

Syntax Description

all	Specifies all interfaces.
interface *type number*	Specifies a particular interface for which to display MAB information.
detail	(Optional) Displays detailed information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

Use the **show mab** command to display information about MAB ports and MAB sessions.

Examples

The following is sample output from the **show mab interface detail** command where a MAB session has been authorized:

```
Switch# show mab interface FastEthernet1/0/1 detail

MAB details for FastEthernet1/0/1
-------------------------------------
Mac-Auth-Bypass           = Enabled
Inactivity Timeout        = None
MAB Client List
---------------
Client MAC                = 000f.23c4.a401
MAB SM state              = TERMINATE
Auth Status               = AUTHORIZED
```

Table 165 describes the significant fields shown in the display.

Table 165 show mab Field Descriptions

Field	Description
Mac-Auth-Bypass	Specifies whether MAB is enabled or disabled.
Inactivity Timeout	The period of time of no activity after which the session is ended.
Client MAC	The MAC address of the client.

Table 165 show mab Field Descriptions (continued)

Field	Description
MAB SM state	The state of the MAB state machine. The possible values, from start to finish, are: • INITIALIZE—the state of the session when it is being initialized. • ACQUIRING—the state of the session when the MAC address is being obtained from the client. • AUTHORIZING—the state of the session when the MAC address is being authorized. • TERMINATE—the state of the session once an authorization result has been obtained.
Auth Status	The authorization status of the MAB session. The possible values are: • AUTHORIZED—the session has been successfully authorized. • UNAUTHORIZED—the session failed to be authorized.

Related Commands

Command	Description
show authentication interface	Displays information about the Auth Manager for a given interface.
show authentication registrations	Displays information about authentication methods registered with the Auth Manager.
show authentication sessions	Displays information about Auth Manager sessions.

show mac access-group interface

To display the ACL configuration on a Layer 2 interface, use the **show mac access-group interface** command.

show mac access-group interface [*interface interface-number*]

Syntax Description

interface	(Optional) Specifies the interface type; valid values are **gigabitethernet**, **tengigabitethernet**, **longreachethernet**, and **port-channel**.
interface-number	(Optional) Specifies the port number.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(33)SXH	Support for this command was introduced.
12.2(33)SRB	Support for this command was introduced.
12.2(33)SRD3	Support for this command was introduced.

Usage Guidelines

The valid values for the port number depend on the chassis used.

Examples

This example shows how to display the ACL configuration on interface fast 6/1:

```
Switch# show mac access-group interface gigabitethernet 6/1
Interface FastEthernet6/1:
   Inbound access-list is simple-mac-acl
   Outbound access-list is not set
```

Related Commands

Command	Description
access-group mode	Specifies the override modes (for example, VACL overrides PACL) and the non-override modes (for example, merge or strict mode).

show mac-address-table

To display the MAC address table, use the **show mac-address-table** command in privileged EXEC mode.

Cisco 2600, 3600, and 3700 Series Routers

show mac-address-table [**secure** | **self** | **count**] [**address** *mac-addr*] [**interface** *type/number*] [**fa** | **gi** *slot/port*] [**atm** *slot/port*] [**vlan** *vlan-id*]

Catalyst 4500 Series Switches

show mac-address-table {**assigned** | **ip** | **ipx** | **other**}

Catalyst 6000/6500 Series Switches and 7600 Series Routers

show mac-address-table [**address** *mac-addr* [**all** | **interface** *type/number* | **module** *number* | **vlan** *vlan-id*] | [**count** [**module** *number* | **vlan** *vlan-id*]] | [**interface** *type/number*] | [**limit** [**vlan** *vlan-id* | **module** *number* | **interface** *interface-type*]] | [**module** *number*] | [**multicast** [**count** | {**igmp-snooping** | **mld-snooping** [**count**] | **user** [**count**] | **vlan** *vlan-id*}]] | [**notification** {**mac-move** [**counter** [*vlan*] | **threshold** | **change**} [**interface** [*interface-number*]]] | [**synchronize statistics**] | [**unicast-flood**] | **vlan** *vlan-id* [**module** *number*]]

Syntax Description

secure	(Optional) Displays only the secure addresses.
self	(Optional) Displays only addresses added by the switch itself.
count	(Optional) Displays the number of entries that are currently in the MAC address table.
address *mac-addr*	(Optional) Displays information about the MAC address table for a specific MAC address. See the "Usage Guidelines" section for formatting information.
interface *type/number*	(Optional) Displays addresses for a specific interface. For the Catalyst 6500 and 6000 series switches, valid values are **atm**, **fastethernet**, **gigabitethernet**, and **port-channel**. For the Cisco 7600 series, valid values are **atm**, **ethernet**, **fastethernet**, **ge-wan**, **gigabitethernet**, **tengigabitethernet**, and **pos**.
fa	(Optional) Specifies Fast Ethernet.
gi	(Optional) Specifies Gigabit Ethernet.
slot/port	(Optional) Adds dynamic addresses to the module in slot 1 or 2. The **/** is required.
atm *slot/port*	(Optional) Adds dynamic addresses to ATM module *slot/port*. Use 1 or 2 for the slot number. Use 0 as the port number. The **/** is required.
vlan *vlan-id*	(Optional) Displays addresses for a specific VLAN. For the Cisco 2600, 3600, and 3700 series, valid values are from 1 to 1005; do not enter leading zeroes. Beginning with Cisco IOS Release 12.4(15)T, the valid VLAN ID range is from 1 to 4094. For the Catalyst 6500 and 6000 series switches and 7600 series, valid values are from 1 to 4094.
assigned	Specifies the assigned protocol entries.

ip	Specifies the IP protocol entries.
ipx	Specifies the IPX protocol entries.
other	Specifies the other protocol entries.
all	(Optional) Displays every instance of the specified MAC address in the forwarding table.
type/number	(Optional) Module and interface number.
module *number*	(Optional) Displays information about the MAC address table for a specific Distributed Forwarding Card (DFC) module.
limit	Displays MAC-usage information.
multicast	Displays information about the multicast MAC address table entries only.
igmp-snooping	Displays the addresses learned by Internet Group Management Protocol (IGMP) snooping.
mld-snooping	Displays the addresses learned by Multicast Listener Discover version 2 (MLDv2) snooping.
user	Displays the manually entered (static) addresses.
notification mac-move	Displays the MAC-move notification status.
notification mac-move counter	(Optional) Displays the number of times a MAC has moved and the number of these instances that have occurred in the system.
vlan	(Optional) Specifies a VLAN to display. For the Catalyst 6500 and 6000 series switches and 7600 series, valid values are from 1 to 4094.
notification threshold	Displays the Counter-Addressable Memory (CAM) table utilization notification status.
notification change	Displays the MAC notification parameters and history table.
synchronize statistics	Displays information about the statistics collected on the switch processor or DFC.
unicast-flood	Displays unicast-flood information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2(8)SA	This command was introduced.
11.2(8)SA3	The **self**, **aging-time**, **count**, and **vlan** *vlan-id* keywords and arguments were added.
11.2(8)SA5	The **atm** *slot/port* keyword and arguments were added.
12.2(2)XT	This command was implemented on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.1(8a)EW	This command was implemented on Catalyst 4500 series switches.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.2(14)SX	This command was implemented on the Supervisor Engine 720.

Release	Modification
12.2(17a)SX	For the Catalyst 6500 and 6000 series switches and 7600 series, this command was changed to support the following optional keywords and arguments: • **unicast-flood** • **count module** *number* • **limit** [**vlan** *vlan-id* | **port** *number* | **interface** *interface-type*] • **notification threshold**
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(18)SXE	For the Catalyst 6500 and 6000 series switches and 7600 series, this command was changed to support the **mld-snooping** keyword on the Supervisor Engine 720 only.
12.2(18)SXF	For the Catalyst 6500 and 6000 series switches and 7600 series, this command was changed to support the **synchronize statistics** keywords on the Supervisor Engine 720 only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)T	This command was modified to extend the range of valid VLAN IDs to 1 to 4094 for specified platforms.
12.2(33)SXH	The **change** keyword was added.
12.2(33)SXI	This command was changed to add the **counter** keyword.

Usage Guidelines

Cisco 2600, 3600, and 3700 Series Routers

This command displays the MAC address table for the switch. Specific views can be defined by using the optional keywords and arguments. If more than one optional keyword is used, then all the conditions must be true for that entry to be displayed.

Catalyst 4500 Series Switches

For the MAC address table entries that are used by the routed ports, the routed port name, rather than the internal VLAN number, is displayed in the “vlan” column.

Catalyst 6500 and 6000 Series Switches and 7600 Series Routers

If you do not specify a module number, the output of the **show mac-address-table** command displays information about the supervisor engine. To display information about the MAC address table of the DFCs, you must enter the module number or the **all** keyword.

The *mac-addr* value is a 48-bit MAC address. The valid format is H.H.H.

The *interface-number* argument designates the module and port number. Valid values depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The optional **module** *number* keyword and argument are supported only on DFC modules. The **module** *number* keyword and argument designate the module number.

Valid values for the *mac-group-address* argument are from 1 to 9.

The optional **count** keyword displays the number of multicast entries.

The optional **multicast** keyword displays the multicast MAC addresses (groups) in a VLAN or displays all statically installed or IGMP snooping-learned entries in the Layer 2 table.

The information that is displayed in the **show mac-address-table unicast-flood** command output is as follows:

- Up to 50 flood entries, shared across all the VLANs that are not configured to use the filter mode, can be recorded.
- The output field displays are defined as follows:
  - ALERT—Information is updated approximately every 3 seconds.
  - SHUTDOWN—Information is updated approximately every 3 seconds.

Note The information displayed on the destination MAC addresses is deleted as soon as the floods stop after the port shuts down.

  - Information is updated each time that you install the filter. The information lasts until you remove the filter.

The dynamic entries that are displayed in the Learn field are always set to Yes.

The **show mac-address-table limit** command output displays the following information:

- The current number of MAC addresses.
- The maximum number of MAC entries that are allowed.
- The percentage of usage.

The **show mac-address-table synchronize statistics** command output displays the following information:

- Number of messages processed at each time interval.
- Number of active entries sent for synchronization.
- Number of entries updated, created, ignored, or failed.

Examples

Cisco 2600, 3600, and 3700 Series Routers

The following is sample output from the **show mac-address-table** command:

```
Router# show mac-address-table

Dynamic Addresses Count:                9
Secure Addresses (User-defined) Count: 0
Static Addresses (User-defined) Count: 0
System Self Addresses Count:           41
Total MAC addresses:                   50
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
0010.0de0.e289       Dynamic          1  FastEthernet0/1
0010.7b00.1540       Dynamic          2  FastEthernet0/5
0010.7b00.1545       Dynamic          2  FastEthernet0/5
0060.5cf4.0076       Dynamic          1  FastEthernet0/1
0060.5cf4.0077       Dynamic          1  FastEthernet0/1
0060.5cf4.1315       Dynamic          1  FastEthernet0/1
0060.70cb.f301       Dynamic          1  FastEthernet0/1
```

```
00e0.1e42.9978       Dynamic          1  FastEthernet0/1
00e0.1e9f.3900       Dynamic          1  FastEthernet0/1
```

Catalyst 4500 Series Switches

This example shows how to display the MAC address table entries that have a specific protocol type (in this case, "assigned"):

```
Switch# show mac-address-table protocol assigned

vlan   mac address     type    protocol  qos             ports
-----+---------------+--------+---------+---+--------------------------------
 200  0050.3e8d.6400  static   assigned  --  Switch
 100  0050.3e8d.6400  static   assigned  --  Switch
   5  0050.3e8d.6400  static   assigned  --  Switch
4092  0000.0000.0000  dynamic  assigned  --  Switch
   1  0050.3e8d.6400  static   assigned  --  Switch
   4  0050.3e8d.6400  static   assigned  --  Switch
4092  0050.f0ac.3058  static   assigned  --  Switch
4092  0050.f0ac.3059  dynamic  assigned  --  Switch
   1  0010.7b3b.0978  dynamic  assigned  --  Fa5/9
Switch#
```

This example shows the "other" output for the previous example:

```
Switch# show mac-address-table protocol other

Unicast Entries
 vlan   mac address     type        protocols               port
-------+---------------+--------+---------------------+--------------------
   1    0000.0000.0201   dynamic other                  FastEthernet6/15
   1    0000.0000.0202   dynamic other                  FastEthernet6/15
   1    0000.0000.0203   dynamic other                  FastEthernet6/15
   1    0000.0000.0204   dynamic other                  FastEthernet6/15
   1    0030.94fc.0dff    static ip,ipx,assigned,other  Switch
   2    0000.0000.0101   dynamic other                  FastEthernet6/16
   2    0000.0000.0102   dynamic other                  FastEthernet6/16
   2    0000.0000.0103   dynamic other                  FastEthernet6/16
   2    0000.0000.0104   dynamic other                  FastEthernet6/16
Fa6/1   0030.94fc.0dff    static ip,ipx,assigned,other  Switch
Fa6/2   0030.94fc.0dff    static ip,ipx,assigned,other  Switch
Multicast Entries
 vlan    mac address     type    ports
-------+---------------+-------+-----------------------------------------------
   1    ffff.ffff.ffff   system Switch,Fa6/15
   2    ffff.ffff.ffff   system Fa6/16
1002    ffff.ffff.ffff   system
1003    ffff.ffff.ffff   system
1004    ffff.ffff.ffff   system
1005    ffff.ffff.ffff   system
Fa6/1   ffff.ffff.ffff   system Switch,Fa6/1
Fa6/2   ffff.ffff.ffff   system Switch,Fa6/2
Switch#
```

Catalyst 6500 and 6000 Series Switches and Cisco 7600 Series Routers

The following is sample output from the **show mac-address-table** command:

```
Switch# show mac-address-table

Dynamic Addresses Count:                9
Secure Addresses (User-defined) Count: 0
Static Addresses (User-defined) Count: 0
System Self Addresses Count:           41
```

```
Total MAC addresses:                  50
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
0010.0de0.e289       Dynamic          1  FastEthernet0/1
0010.7b00.1540       Dynamic          2  FastEthernet0/5
0010.7b00.1545       Dynamic          2  FastEthernet0/5
0060.5cf4.0076       Dynamic          1  FastEthernet0/1
0060.5cf4.0077       Dynamic          1  FastEthernet0/1
0060.5cf4.1315       Dynamic          1  FastEthernet0/1
0060.70cb.f301       Dynamic          1  FastEthernet0/1
00e0.1e42.9978       Dynamic          1  FastEthernet0/1
00e0.1e9f.3900       Dynamic          1  FastEthernet0/1
```

Note In a distributed Encoded Address Recognition Logic (EARL) switch, the asterisk (*) indicates a MAC address that is learned on a port that is associated with this EARL.

This example shows how to display the information about the MAC address table for a specific MAC address with a Supervisor Engine 720:

```
Router# show mac-address-table address 001.6441.60ca

Codes: * - primary entry

  vlan   mac address     type    learn qos            ports
------+----------------+--------+-----+---+--------------------------
Supervisor:
*  ---  0001.6441.60ca    static  No    --  Router
```

This example shows how to display MAC address table information for a specific MAC address with a Supervisor Engine 720:

```
Router# show mac-address-table address 0100.5e00.0128

Legend: * - primary entry
        age - seconds since last seen
        n/a - not available

  vlan   mac address     type    learn     age              ports
------+----------------+--------+-----+----------+--------------------------
Supervisor:
*   44  0100.5e00.0128    static  Yes          -   Fa6/44,Router
*    1  0100.5e00.0128    static  Yes          -   Router
Module 9:
*   44  0100.5e00.0128    static  Yes          -   Fa6/44,Router
*    1  0100.5e00.0128    static  Yes          -   Router
```

This example shows how to display the currently configured aging time for all VLANs:

```
Router# show mac-address-table aging-time

Vlan    Aging Time
----    ----------
*100     300
200     1000
```

This example shows how to display the entry count for a specific slot:

```
Router# show mac-address-table count module 1

MAC Entries on slot 1 :
Dynamic Address Count:                4
Static Address (User-defined) Count:  25
Total MAC Addresses In Use:           29
Total MAC Addresses Available:        131072
```

This example shows how to display the information about the MAC address table for a specific interface with a Supervisor Engine 720:

```
Router# show mac-address-table interface fastethernet 6/45

Legend: * - primary entry
        age - seconds since last seen
        n/a - not available

  vlan   mac address     type    learn     age              ports
------+----------------+--------+-----+----------+--------------------------
*   45  00e0.f74c.842d   dynamic  Yes          5   Fa6/45
```

Note A leading asterisk (*) indicates entries from a MAC address that was learned from a packet coming from an outside device to a specific module.

This example shows how to display the limit information for a specific slot:

```
Router# show mac-address-table limit vlan 1 module 1
vlan    switch   module    action      maximum  Total entries  flooding
-------+--------+---------+-----------+--------+--------------+------------
1          1        7       warning      500      0              enabled
1          1        11      warning      500      0              enabled
1          1        12      warning      500      0              enabled

Router#show mac-address-table limit vlan 1 module 2
vlan    switch   module    action      maximum  Total entries  flooding
-------+--------+---------+-----------+--------+--------------+------------
1          2         7      warning      500      0              enabled
1          2         9      warning      500      0              enabled
```

The following example shows how to display the MAC-move notification status:

```
Router# show mac-address-table notification mac-move
MAC Move Notification: Enabled
Router#
```

The following example shows how to display the MAC move statistics:

```
Router> show mac-address-table notification mac-move counter
--------------------------------------------------------------------------------
Vlan Mac Address From Mod/Port To Mod/Port Count
---- ----------------- ---------------------- ---------------------- ------------
1 00-01-02-03-04-01 2/3 3/1 10
20 00-01-05-03-02-01 5/3 5/1 20
```

This example shows how to display the CAM-table utilization-notification status:

```
Router# show mac-address-table notification threshold

Status limit Interval
-------------+-----------+-------------
enabled 1 120
```

This example shows how to display the MAC notification parameters and history table:

```
Router# show mac-address-table notification change

MAC Notification Feature is Disabled on the switch
MAC Notification Flags For All Ethernet Interfaces :
--------------------------------------------------
Interface                   MAC Added Trap MAC Removed Trap
--------------------         -------------- ----------------
```

This example shows how to display the MAC notification parameters and history table for a specific interface:

```
Router# show mac-address-table notification change interface gigabitethernet5/2

MAC Notification Feature is Disabled on the switch
Interface                   MAC Added Trap MAC Removed Trap
--------------------         -------------- ----------------
GigabitEthernet5/2           Disabled       Disabled
```

This example shows how to display unicast-flood information:

```
Router# show mac-address-table unicast-flood

> > Unicast Flood Protection status: enabled
> >
> > Configuration:
> > vlan Kfps action timeout
> > ------+----------+-----------------+----------
> > 2 2 alert none
> >
> > Mac filters:
> > No. vlan source mac addr. installed
> > on time left (mm:ss)
> >
> >-----+------+-----------------+------------------------------+------------------
> >
> > Flood details:
> > Vlan source mac addr. destination mac addr.
> >
> >------+---------------+-------------------------------------------------
> > 2 0000.0000.cafe 0000.0000.bad0, 0000.0000.babe,
> > 0000.0000.bac0
> > 0000.0000.bac2, 0000.0000.bac4,
> > 0000.0000.bac6
> > 0000.0000.bac8
> > 2 0000.0000.caff 0000.0000.bad1, 0000.0000.babf,
> > 0000.0000.bac1
> > 0000.0000.bac3, 0000.0000.bac5,
> > 0000.0000.bac7
> > 0000.0000.bac9
```

This example shows how to display the information about the MAC-address table for a specific VLAN:

```
Router# show mac-address-table vlan 100

vlan   mac address     type    protocol  qos             ports
-----+---------------+--------+---------+---+--------------------------------
 100  0050.3e8d.6400  static   assigned  --  Router
 100  0050.7312.0cff  dynamic        ip  --  Fa5/9
 100  0080.1c93.8040  dynamic        ip  --  Fa5/9
 100  0050.3e8d.6400  static        ipx  --  Router
 100  0050.3e8d.6400  static      other  --  Router
 100  0100.0cdd.dddd  static      other  --  Fa5/9,Router,Switch
 100  00d0.5870.a4ff  dynamic        ip  --  Fa5/9
 100  00e0.4fac.b400  dynamic        ip  --  Fa5/9
 100  0100.5e00.0001  static         ip  --  Fa5/9,Switch
 100  0050.3e8d.6400  static         ip  --  Router
```

This example shows how to display the information about the MAC address table for MLDv2 snooping:

```
Router# show mac-address-table multicast mld-snooping

vlan mac address type learn qos ports
-----+---------------+--------+-----+---+--------------------------------
--- 3333.0000.0001 static Yes - Switch,Stby-Switch
--- 3333.0000.000d static Yes - Fa2/1,Fa4/1,Router,Switch
--- 3333.0000.0016 static Yes - Switch,Stby-Switch
```

Related Commands

Command	Description
clear mac-address-table	Deletes entries from the MAC address table.
mac-address-table aging-time	Configures the aging time for entries in the Layer 2 table.
mac-address-table limit	Enables MAC limiting.
mac-address-table notification mac-move	Enables MAC-move notification.
mac-address-table static	Adds static entries to the MAC address table or configures a static MAC address with IGMP snooping disabled for that address.
mac-address-table synchronize	Synchronizes the Layer 2 MAC address table entries across the PFC and all the DFCs.
show mac-address-table static	Displays static MAC address table entries only.

show management-interface

To display information about management interfaces, use the **show management-interface** command in privileged EXEC mode.

show management-interface [*interface* | **protocol** *protocol-name*]

Syntax Description

interface	(Optional) Interface for which you want to view information.
protocol	(Optional) Indicates that a protocol is specified.
protocol-name	(Optional) Protocol for which you want to view information.

Command Default

Information about all dedicated management interfaces is displayed when no interface or protocol is specified.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The **show management-interface** command allows you to view all management interface configurations and activity on a device and to filter the output by interface or protocol. This flexibility is useful for network monitoring and troubleshooting.

Examples

The following sample output is from a **show management-interface** command when no interface or protocol is specified:

```
Router# show management-interface

Management interface FastEthernet0/0
        Protocol        Packets processed
             ssh                223981
```

The following sample output is from a **show management-interface** command with interface FastEthernet 0/0 specified:

```
Router# show management-interface fastEthernet 0/0

Management interface FastEthernet0/0
        Protocol        Packets processed
             ssh                223981
```

The following sample output is from a **show management-interface** command with protocol Secure Shell (SSH) specified:

```
Router# show management-interface protocol ssh

The following management-interfaces allow protocol ssh
        FastEthernet0/0 Packets processed 223981
```

Table 166 describes the significant fields shown in the displays.

Table 166 show management-interface Field Descriptions

Field	Description
Management interface <interface>	Interface designated as a management interface.
Protocol	Network management protocols enabled on the interface.
Packets processed	The number of packets processed on the interface.

Related Commands

Command	Description
management-interface allow	Configures an interface to accept only network management packets.

show mls rate-limit

To display information about the MLS rate limiter in the EXEC command mode, use the **show mls rate-limit** command.

show mls rate-limit [**usage**]

Syntax Description

usage	(Optional) Displays the feature that is used with the rate-limiter register.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	The command output was changed to include hardware rate-limiting status.
12.2(17b)SXA	The command output was changed to display a hyphen (-) instead of an asterisk (*) to indicate that the multicast partial-SC rate limiter is disabled.
12.2(18)SXD	The command output was changed to display IPv6 information.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

In the command output, the rate-limit status could be one of the following:

- On indicates a rate for that particular case has been set.
- Off indicates that the rate-limiter type has not been configured, and the packets for that case are not rate limited.
- On/Sharing indicates a particular case (not manually configured) is affected by the configuration of another rate limiter belonging to the same sharing group.
- A hyphen indicates that the multicast partial-SC rate limiter is disabled.

In the command output, the rate-limit sharing indicates the following information:

- Whether sharing is static or dynamic
- Group dynamic sharing codes

The **show mls rate-limit usage** command displays the hardware register that is used by a rate-limiter type. If the register is not used by any rate-limiter type, Free is displayed in the output. If the register is used by a rate-limiter type, Used and the rate-limiter type are displayed.

Examples

This example shows how to display information about the rate-limit status:

```
Router# show mls rate-limit
Sharing Codes: S - static, D - dynamic
 Codes dynamic sharing: H - owner (head) of the group, g - guest of the group

   Rate Limiter Type       Status     Packets/s   Burst  Sharing
 ---------------------   ----------   ---------   -----  -------
         MCAST NON RPF   Off                  -       -     -
        MCAST DFLT ADJ   On              100000     100  Not sharing
      MCAST DIRECT CON   Off                  -       -     -
        ACL BRIDGED IN   Off                  -       -     -
       ACL BRIDGED OUT   Off                  -       -     -
           IP FEATURES   Off                  -       -     -
          ACL VACL LOG   On                2000       1  Not sharing
            MAC PBF IN   Off                  -       -     -
           CEF RECEIVE   Off                  -       -     -
             CEF GLEAN   Off                  -       -     -
      MCAST PARTIAL SC   On               100000     100  Not sharing
        IP RPF FAILURE   On                  100      10  Group:0 S
           TTL FAILURE   Off                  -       -     -
 ICMP UNREAC. NO-ROUTE   On                  100      10  Group:0 S
 ICMP UNREAC. ACL-DROP   On                  100      10  Group:0 S
         ICMP REDIRECT   Off                  -       -     -
           MTU FAILURE   Off                  -       -     -
       MCAST IP OPTION   Off                  -       -     -
       UCAST IP OPTION   Off                  -       -     -
           LAYER_2 PDU   Off                  -       -     -
            LAYER_2 PT   Off                  -       -     -
      LAYER_2 PORTSEC    Off                  -       -     -
    LAYER_2 MiniProto    Off                  -       -     -
     DHCP Snooping IN    Off                  -       -     -
    DHCP Snooping OUT    Off                  -       -     -
       ARP Inspection    Off                  -       -     -
            IP ERRORS    On                   100      10  Group:0 S
          CAPTURE PKT    Off                  -       -     -
           MCAST IGMP    Off                  -       -     -
 MCAST IPv6 DIRECT CON   Off                  -       -     -
 MCAST IPv6 ROUTE CNTL   Off                  -       -     -
 MCAST IPv6 *G M BRIDG   Off                  -       -     -
  MCAST IPv6 SG BRIDGE   Off                  -       -     -
  MCAST IPv6 DFLT DROP   Off                  -       -     -
 MCAST IPv6 SECOND. DR   Off                  -       -     -
  MCAST IPv6 *G BRIDGE   Off                  -       -     -
       MCAST IPv6 MLD    Off                  -       -     -
  IP ADMIS. ON L2 PORT   Off                  -       -     -
       MCAST IPv4 PIM    Off                  -       -     -
Router#
```

This example shows how to display information about the rate-limit usage:

```
Router # show mls rate-limit usage
Rate Limiter Type     Packets/s   Burst
                      ----------------------   ---------   -----
Layer3 Rate Limiters:
             RL# 0: Free                        -           -       -
             RL# 1: Free                        -           -       -
             RL# 2: Free                        -           -       -
             RL# 3: Free                        -           -       -
             RL# 4: Free                        -           -       -
             RL# 5: Used
                                 IP RPF FAILURE         100      10
                              ICMP UNREAC. NO-ROUTE     100      10
                              ICMP UNREAC. ACL-DROP     100      10
```

```
                                        IP ERRORS          100       10
             RL# 6: Used
                                    ACL VACL LOG         2000        1
             RL# 7: Used
                                  MCAST DFLT ADJ       100000      100
             RL# 8: Rsvd for capture            -            -        -

Layer2 Rate Limiters:
             RL# 9: Reserved
             RL#10: Reserved
                                MCAST PARTIAL SC       100000      100
             RL#11: Free                        -            -        -
             RL#12: Free                        -            -        -
Router #
```

Related Commands

Command	Description
mls rate-limit multicast ipv4	Enables and sets the rate limiters for the IPv4 multicast packets.
mls rate-limit multicast ipv6	Configures the IPv6 multicast rate limiters.
mls rate-limit unicast acl	Enables and sets the ACL-bridged rate limiters.

show monitor event-trace dmvpn

To display Dynamic Multipoint VPN (DMVPN) trace information, use the **show monitor event-trace dmvpn** command in privileged EXEC mode.

show monitor event-trace dmvpn [**merged** | **nhrp** {**event** | **error** | **exception**} | **tunnel** [**parameters**]] {**all** | **back** *time* | **clock** *hh*:*mm* [*day month* | *month day*] | **from-boot** [*boot-time*] | **latest**} [**detail**]

Syntax Description

merged	(Optional) Displays all traces in the current buffer.
nhrp	(Optional) Displays Next Hop Resolution Protocol (NHRP) traces.
event	(Optional) Displays NHRP event traces.
error	(Optional) Displays NHRP error traces.
exception	(Optional) Displays NHRP exception traces.
tunnel	(Optional) Displays tunnel events.
parameters	(Optional) Displays parameters of the trace.
all	Displays all traces in the current buffer.
back *time*	Displays traces since the specified time. Time can be specified as minutes (*mmm*) or in hour:minute (*hh*:*mm*) format.
clock *hh*:*mm*	Displays trace from the specified time.
day	(Optional) Day in a month.
month	(Optional) Month of a year.
from-boot	Displays trace after the specified time after boot.
boot-time	(Optional) Time specified to wait to display trace after boot.
latest	Displays the latest trace events since the previous display.
detail	(Optional) Displays detailed trace information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(4)M	This command was introduced.

Usage Guidelines

You can use the **show monitor event-trace dmvpn** command to verify DMVPN event tracing.

This command displays all the tunnel events, including the DMVPN tunnel events and the non-DMVPN tunnel events.

Note The **show monitor event-trace dmvpn** command output displays all tunnel events. You dare not able to filter only the DMVPN tunnel information in the display.

Examples

The following is sample output from the **show monitor event-trace dmvpn nhrp exception all** command. The fields in the display are self-explanatory.

```
Router# show monitor event-trace dmvpn nhrp exception all

ev_type : NHS-UP trace_type: NHRP-EXCEPTION

*May 17 05:00:09.999: NHRP-EXCEPTION:NHS-UP  Tunnel0 : NHS UP,
(VPN DEST )10.0.0.251 -> (NBMA DEST)172.16.0.251,
(VPN SRC)10.0.0.1 -> (NBMA SRC)172.16.0.1

ev_type : NHS-DOWN trace_type: NHRP-EXCEPTION

*May 17 05:00:09.999: NHRP-EXCEPTION:NHS-DOWN  Tunnel0 : NHS DOWN,
(VPN DEST )10.0.0.251 -> (NBMA DEST)172.16.0.251,
(VPN SRC)10.0.0.1 -> (NBMA SRC)172.16.0.1, reason: External

ev_type : NHC-UP trace_type: NHRP-EXCEPTION

*May 17 05:00:09.999: NHRP-EXCEPTION:NHC-UP  Tunnel0 : NHC UP,
(VPN DEST )10.0.0.251 -> (NBMA DEST)172.16.0.251,
(VPN SRC)10.0.0.1 -> (NBMA SRC)172.16.0.1

ev_type : NHC-DOWN trace_type: NHRP-EXCEPTION

*May 17 05:00:09.999: NHRP-EXCEPTION:NHC-DOWN  Tunnel0 : NHC DOWN,
(VPN DEST )10.0.0.251 -> (NBMA DEST)172.16.0.251,
(VPN SRC)10.0.0.1 -> (NBMA SRC)172.16.0.1, reason: External

ev_type : NHP-UP trace_type: NHRP-EXCEPTION

*May 17 05:00:09.999: NHRP-EXCEPTION:NHP-UP  Tunnel0 : NHP UP,

(VPN DEST )10.0.0.251 -> (NBMA DEST)172.16.0.251,
(VPN SRC)10.0.0.1 -> (NBMA SRC)172.16.0.1

ev_type : NHP-DOWN trace_type: NHRP-EXCEPTION

*May 17 05:00:09.999: NHRP-EXCEPTION:NHP-DOWN  Tunnel0 : NHP DOWN,
(VPN DEST )10.0.0.251 -> (NBMA DEST)172.16.0.251,
(VPN SRC)10.0.0.1 -> (NBMA SRC)172.16.0.1, reason: External

ev_type : NHRP-RATE_LIMIT trace_type: NHRP-EXCEPTION

*May 17 05:00:09.999: NHRP-EXCEPTION:NHRP-RATE_LIMIT  Tunnel0 : Max-send Quota of
10000pkts/500sec exceeded

ev_type : NHS-RECOVERY-NHS-STATE trace_type: NHRP-EXCEPTION

*May 17 05:00:09.999: NHRP-EXCEPTION:NHS-RECOVERY-NHS-STATE  NHS recovery event string
```

Related Commands

Command	Description
monitor event-trace dmvpn	Monitors and controls DMVPN traces.

show object-group

To display information about object groups that are configured, use the **show object-group** command in user EXEC or privileged EXEC mode.

show object-group [*object-group-name* | **network** | **service**]

Syntax Description

object-group-name	(Optional) Name of an object group for which information will be displayed.
network | **service**	(Optional) Indicates whether to display information for all network object groups or all service object groups.

Command Default

Information is displayed for all object groups.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following is sample output from the **show object-group** command:

```
Router# show object-group
Network object group auth_proxy_acl_deny_dest
 host 171.68.225.134

Service object group auth_proxy_acl_deny_services
 tcp eq www
 tcp eq 443

Network object group auth_proxy_acl_permit_dest
 10.34.250.96 255.255.255.224
 171.68.0.0 255.252.0.0
 172.16.0.0 255.240.0.0
 128.107.0.0 255.255.0.0
 10.0.0.0 255.0.0.0
 64.100.0.0 255.253.0.0
 64.104.0.0 255.255.0.0
 144.254.0.0 255.255.0.0
 161.44.0.0 255.255.0.0
 192.168.0.0 255.255.0.0

Service object group auth_proxy_acl_permit_services
 tcp eq www
 tcp eq 443
```

Table 167 describes the significant fields shown in the displays.

Table 167 show object-group Field Descriptions

Field	Description
Network object group auth_proxy_acl_deny_dest	Name of the network object group.
host 171.68.225.134	IP address of the host object.
Network object group auth_proxy_acl_deny_services	Name of the service object group.
tcp eq www tcp eq 443	TCP port types.
10.34.250.96 255.255.255.224	Network address and network mask of the subnet object.

Related Commands

Command	Description
deny	Sets conditions in a named IP access list or OGACL that will deny packets.
ip access-group	Applies an ACL or OGACL to an interface or a service policy map.
ip access-list	Defines an IP access list or OGACL by name or number.
object-group network	Defines network object groups for use in OGACLs.
object-group service	Defines service object groups for use in OGACLs.
permit	Sets conditions in a named IP access list or OGACL that will permit packets.
show ip access-list	Displays the contents of IP access lists or OGACLs.

show parameter-map type consent

To display consent parameter map information, use the **show parameter-map type consent** command in privileged EXEC mode.

show parameter-map type consent [*parameter-map-name* | **default**]

Syntax Description

parameter-map-name	(Optional) Name of the parameter map.
default	(Optional) Specifies default consent parameter map information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(20)T	The command was modified. The *parameter-map-name* argument was added.

Examples

The following is sample output from the **show parameter-map type consent** command. The fields are self-explanatory.

```
Router# show parameter-map type consent

parameter-map type consent map1
    Syslog : Enabled
    File download time(in minutes) : 456
    Number of Accepted Users : 0
    Number of Denied Users : 0
```

show parameter-map type inspect

To display user-configured or default inspect type parameter maps, use the **show parameter-map type inspect** command in privileged EXEC mode.

show parameter-map type inspect [**default** | **global**]

Syntax Description

default	(Optional) Displays the default inspect type parameter map values. **Note** Use this keyword when no parameter map is attached to the inspect action.
global	(Optional) Displays the default inspect type parameter map values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.1(1)T	The **global** keyword was added.

Examples

The following is sample output from the **show parameter-map type inspect** command. The field descriptions are self-explanatory.

```
Router# show parameter-map type inspect

audit-trail off
 alert on
 max-incomplete low 2147483647
 max-incomplete high 2147483647
 one-minute low 2147483647
 one-minute high 2147483647
 udp idle-time 30
 icmp idle-time 10
 dns-timeout 5
 tcp idle-time 3600
 tcp finwait-time 5
 tcp synwait-time 30
 tcp max-incomplete host 4294967295 block-time 0
 sessions maximum 2147483647
```

The following is sample output with the **default** keyword. The field descriptions are self-explanatory.

```
Router# show parameter-map type inspect default

parameter-map type inspect default values
 audit-trail off
 alert on
 max-incomplete low unlimited
 max-incomplete high unlimited
 one-minute low unlimited
 one-minute high unlimited
 udp idle-time 30
 icmp idle-time 10
```

```
 dns-timeout 5
 tcp idle-time 3600
 tcp finwait-time 5
 tcp synwait-time 30
 tcp max-incomplete host 50 block-time 0
```

The following is sample output with the **global** keyword. The field descriptions are self-explanatory.

```
Router# show parameter-map type inspect global

alert on
 sessions maximum 2147483647
 waas disabled
 l2-transparent dhcp-passthrough disabled
 log dropped-packets disabled
 log summary disabled
 max-incomplete low 2147483647
 max-incomplete high 2147483647
 one-minute low 2147483647
 one-minute high 2147483647
```

show parameter-map type protocol-info

To display protocol parameter map information, use the **show parameter-map type protocol-info** command in privileged EXEC mode.

show parameter-map type protocol-info [*parameter-map-name* [**dns-cache**] | **dns-cache** | **msrpc** | **zone-pair** *zone-pair-name* | **stun-ice** [*parameter-map-name*]]

Syntax Description

parameter-map-name	(Optional) Name of the parameter map.
dns-cache	(Optional) Displays the protocol information about the Domain Name System (DNS) cache.
msrpc	(Optional) Displays the protocol information about the Microsoft Remote Procedure Call (MSRPC) parameter map.
zone-pair *zone-pair-name*	(Optional) Specifies the name of the zone pair.
stun-ice	(Optional) Displays the protocol information of Session Traversal Utilities for Network Address Translation (NAT) and Interactive Connectivity Establishment (STUN-ICE). STUN is an Internet standards-track suite of methods, including a network protocol, used in NAT traversal for applications of real-time voice, video, messaging, and other interactive IP communications. ICE is a technique used in computer networking involving NATs in Internet applications of VoIP, peer-to-peer communications, video, instant messaging, and other interactive media. In such applications, NAT traversal is an important component to facilitate communications involving hosts on private network installations, which often are located behind firewalls.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.4(22)T	The command was modified. The **stun-ice** keyword was added.
15.1(4)M	This command was modified. The **msrpc** keyword was added.

Examples

The following is sample output from the **show parameter-map type protocol-info** command. The fields are self-explanatory.

```
Router# show parameter-map type protocol-info

parameter-map type protocol-info map2
  server ip 192.168.1.1
```

Related Commands

Command	Description
parameter-map type protocol-info	Creates or modifies a protocol-specific parameter map and enters parameter-map type configuration mode.

show parameter-map type inspect-vrf

To display information about the configured inspect VPN Routing and Forwarding (VRF) type parameter map, use the **show parameter-map type inspect-vrf** command in user EXEC or privileged EXEC mode.

show parameter-map type inspect-vrf [*name* | **default**]

Syntax Description

name	(Optional) Name of the inspect VRF type parameter map.
default	(Optional) Specifies the default inspect VRF type parameter map.

Command Default

This command has no default settings.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Examples

The following is sample output from the **show parameter-map type inspect-vrf** command:

```
Router# show parameter-map type inspect-vrf vpmap01

  VRF: vrf001, Parameter-Map: vpmap01
       total_session_cnt: 3500
       exceed_cnt:        40
       tcp_half_open_cnt: 3520
       syn_exceed_cnt:    40
```

Table 168 describes the significant fields shown in the display.

Table 168 show parameter-map type inspect-vrf Field Descriptions

Field	Description
total_session_cnt	Total session count.
exceed_cnt	Number of sessions that exceeded the configured session count.
tcp_half_open_cnt	TCP half-open sessions configured for each VRF. When the configured session limit is reached, the TCP synchronization (SYN) cookie verifies the source of the half-open TCP sessions before creating more sessions. A TCP half-open session is a session that has not reached the established state.
syn_exceed_count	Number of SYN packets that exceeded the configured SYN flood rate limit.

Related Commands

Command	Description
parameter-map type inspect-vrf	Configures an inspect VRF type parameter map.

show parameter-map type inspect-zone

To display information about the configured inspect zone-type parameter map, use the **show parameter-map type inspect-zone** command in user EXEC or privileged EXEC mode.

show parameter-map type inspect-zone [*name* | **default**]

Syntax Description

name	(Optional) Name of the inspect zone-type parameter map.
default	(Optional) Specifies the default inspect zone-type parameter map.

Command Default

This command has no default settings.

Command Modes

User EXEC (>)
Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Examples

The following is sample output from the **show parameter-map type inspect-zone** command:

```
Router# show parameter-map type inspect-zone zone-pmap

parameter-map type inspect-zone zone-pmap
 tcp syn-flood-rate 400
 max-destination 10000
```

Table 169 describes the fields shown in the display.

Table 169 show parameter-map type inspect-zone Field Descriptions

Field	Description
parameter-map type inspect-zone	Name of the inspect zone-type parameter map.
tcp syn-flood-rate	TCP synchronization (SYN) flood rate limit. When the configured maximum packet rate is reached, the TCP SYN cookie protection is triggered.
max-destination	Maximum number of destinations that a firewall can track.

Related Commands

Command	Description
parameter-map type inspect-zone	Configures an inspect zone-type parameter map.

show parameter-map type regex

To display regex parameter-map information, use the **show parameter-map type regex** command in privileged EXEC mode.

show parameter-map type regex [*parameter-map-name*]

Syntax Description

parameter-map-type	(Optional) Name of the parameter map.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Examples

The following is sample output from the **show parameter-map type regex** command. The fields are self-explanatory.

```
Router# show parameter-map type regex

parameter-map type regex map3
 pattern x*y
```

show parameter-map type trend-global

To display the parameter map for the global parameters for a Trend Micro URL filtering policy, use the **show parameter-map type trend-global** command in privileged EXEC mode.

show parameter-map type trend-global [*parameter-map-name*] [**default**]

Syntax Description

parameter-map-name	(Optional) The name of the parameter map for which to display parameters.
default	(Optional) Specifies that the default values for the global Trend Micro filtering parameters be displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **show parameter-map type trend-global** command to display the global parameters for Trend Micro URL filtering policies.

Examples

The following is sample output from the **show parameter-map type trend-global default** command:

```
Router# show parameter-map type trend-global default

parameter-map type trend-global default values
   server trps.trendmicro.com http-port 80 https-port 443 retrans 3 timeout 60
   alert on
   cache-size 256 KB
   cache-lifetime 24
```

The following is sample output from the **show parameter-map type trend-global** command when the server name and maximum cache size have been specified in the parameter map Global-Parameters:

```
Router# show parameter-map type trend-global Global-Parameters

parameter-map type trend-global Global-Parameters
   server trps1.example.com http-port 80 https-port 443 retrans 3 timeout 60
   alert on
   cache-size 300 KB
   cache-lifetime 24
```

Related Commands

Command	Description
show parameter-map type urlfpolicy	Displays the parameters for a URL filtering policy.

show parameter-map type urlf-glob

To display the parameter maps for local URL filtering, use the **show parameter-map type urlf-glob** command in privileged EXEC mode.

show parameter-map type urlf-glob [*parameter-map-name*]

Syntax Description

parameter-map-name	(Optional) Name of the URL filtering parameter map to display.

Command Default

The parameter maps for all local URL filtering policies are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **show parameter-map type urlf-glob** command to display the parameter maps for local URL filtering policies.

Examples

The following is sample output from the **show parameter-map type urlf-glob** command when two parameter maps for local URL filtering have been configured:

```
Router# show parameter-map type urlf-glob

parameter-map type urlf-glob trusted-domain-param
 pattern www.example.com
 pattern *.example1.com

parameter-map type urlf-glob untrusted-domain-param
 pattern www.example3.com
 pattern *.example4.com
```

Related Commands

Command	Description
show parameter-map type trend-global	Displays the global parameters for a Trend Micro URL filtering policy.
show parameter-map type urlfpolicy	Displays the parameters for a URL filtering policy.

show parameter-map type urlfilter

Note Effective with Cisco IOS Release 12.4(15)XZ, the **show parameter-map type urlfilter** command is not available in Cisco IOS software.

To display user-configured or default URL filter type parameter maps, use the **show parameter-map type urlfilter** command in privileged EXEC mode.

show parameter-map type urlfilter [**default**]

Syntax Description

default	(Optional) Displays the default urlfilter parameter map values. **Note** If this keyword is not issued, user-configured parameter maps will be displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was removed.

Examples

The following example shows sample output from the **show parameter-map type urlfilter** command:

```
Router# show parameter-map type urlfilter

 parameter-map type urlfilter default values
  urlf-server-log off
  audit-trail off
  alert on
  max-request 1000
  max-resp-pak 200
  source-interface default
  allow-mode off
  cache 5000
```

The following example shows sample output from the **show parameter-map type urlfilter default** command:

```
Router# show parameter-map type urlfilter default

parameter-map type urlfilter default values
 urlf-server-log off
 audit-trail off
 alert on
 max-request 1000
 max-resp-pak 200
 source-interface default
 allow-mode off
 cache 5000
```

show parameter-map type urlfpolicy

To display the parameter maps associated with a URL filtering policy, use the **show parameter-map type urlfpolicy** command in privileged EXEC mode.

show parameter-map type urlfpolicy {**local** | **trend** | **n2h2** | **websense**} [*parameter-map-name*] [**default**]

Syntax Description

local	Specifies that the parameters for local URL filtering policies be displayed.
trend	Specifies that the parameters for Trend Micro URL filtering policies be displayed.
n2h2	Specifies that the parameters for SmartFilter URL filtering policies be displayed.
websense	Specifies that the parameters for Websense URL filtering policies be displayed.
parameter-map-name	(Optional) The name of the parameter map for a URL filtering policy to be displayed.
default	(Optional) Displays the default values for the URL filtering policy. **Note** If this keyword is not issued, user-configured values will be displayed.

Command Default

The parameter maps for all URL filtering policies of the type specified (**local**, **trend**, **n2h2**, or **websense**) are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

The following example shows the default values for a Websense URL filtering policy:

```
Router# show parameter-map type urlfpolicy websense default

 parameter-map type urlfilter websense default values
  urlf-server-log off
  audit-trail off
  alert on
  max-request 1000
  max-resp-pak 200
  source-interface default
  allow-mode off
  cache 5000
```

show parser view

To display command-line interface (CLI) view information, use the **show parser view** command in privileged EXEC mode.

show parser view [**all**]

Syntax Description

all	(Optional) Displays information about all CLI views that are configured on the router.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

The **show parser view** command will display information only about the view that the user is currently in. This command is available for both root view users and lawful intercept view users—except for the **all** keyword, which is available only to root view users. However, the **all** keyword can be configured by a user in root view to be available for users in lawful intercept view.

The **show parser view** command cannot be excluded from any view.

Examples

The following example shows how to display information from the root view and the CLI view “first”:

```
Router# enable view
Router#
01:08:16:%PARSER-6-VIEW_SWITCH:successfully set to view 'root'.
Router#
! Enable the show parser view command from the root view
Router# show parser view
Current view is 'root'
! Enable the show parser view command from the root view to display all views
Router# show parser view all
Views Present in System:
View Name:   first
View Name:   second
! Switch to the CLI view “first.”
Router# enable view first
Router#
01:08:09:%PARSER-6-VIEW_SWITCH:successfully set to view 'first'.
! Enable the show parser view command from the CLI view “first.”
Router# show parser view
Current view is 'first'
```

Related Commands

Command	Description
parser view	Creates or changes a CLI view and enters view configuration mode.

show platform hardware qfp feature

To display feature-specific information in the Cisco Quantum Flow Processor (QFP), use the **show platform hardware qfp feature** command in privileged EXEC mode.

show platform hardware qfp {**active | standby**} **feature alg** {**memory | statistics** [*protocol* **| clear** [**clear**]]}

Syntax Description

active	Displays the active instance of the processor.
standby	Displays the standby instance of the processor.
alg	Displays the Application Level Gateway (ALG) information of the processor.
memory	Displays ALG memory usage information of the processor.
statistics	Displays ALG common statistics information of the processor.
protocol	Protocol name. It can be one of the following values: • **dns** —Displays Domain Name System (DNS) ALG information in the QFP datapath. • **exec**—Displays exec ALG information in the QFP datapath. • **ftp**—Displays FTP ALG information in the QFP datapath. • **h323**—Displays H.323 ALG information in the QFP datapath. • **http**—Displays HTTP ALG information in the QFP datapath. • **imap**—Displays Internet Message Access Protocol (IMAP) ALG information in the QFP datapath. • **ldap**—Displays Lightweight Directory Access Protocol (LDAP) ALG information in the QFP datapath. • **login**—Displays login ALG information in the QFP datapath. • **netbios**—Displays Network Basic Input Output System (NetBIOS) ALG information in the QFP datapath. • **pop3**—Displays pop3 ALG information in the QFP datapath. • **rtsp**—Displays Rapid Spanning Tree Protocol (RSTP) ALG information in the QFP datapath. • **shell**—Displays shell ALG information in the QFP datapath. • **sip**—Displays Session Initiation Protocol (SIP) ALG information in the QFP datapath. • **skinny**—Displays skinny ALG information in the QFP datapath. • **smtp**—Displays Simple Mail Transfer Protocol (SMTP) ALG information in the QFP datapath. • **sunrpc**—Displays Sun RPC ALG information in the QFP datapath. • **tftp**—Displays TFTP ALG information in the QFP datapath.
clear	Clears ALG common counters after display.
clear	(Optional) Clears the ALG counters.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.2	This command was introduced.
Cisco IOS XE Release 3.1S	This command was modified. Support for the NetBIOS protocol was added.
Cisco IOS XE Release 3.2S	This command was modified. The show output was modified to display SIP statistics information.

Usage Guidelines The **show platform hardware qfp feature** command when used with the **netbios** keyword displays the NetBIOS ALG memory usage and statistics information of the processor.

Examples The following example displays the NetBIOS ALG statistics information of the processor:

```
Router# show platform hardware qfp active feature alg statistics netbios

NetBIOS ALG Statistics:
  No. of allocated chunk elements in L7 data pool:0
  No. of times L7 data is allocated:0  No. of times L7 data is freed:0
  Datagram Service statistics
    Total packets            :0
    Direct unique packets    :0
    Direct group packets     :0
    Broadcast packets        :0
    DGM Error packets        :0
    Query request packets    :0
    Positive Qry response packets :0
    Netgative Qry response packets:0
    Unknown packets          :0
    Total error packets      :0
  Name Service statistics
    Total packets            :0
    Query request packets    :0
    Query response packets   :0
    Registration req packets :0
    Registration resp packets:0
    Release request packets  :0
    Release response packets :0
    WACK packets             :0
    Refresh packets          :0
    Unknown packets          :0
    Total error packets      :0
  Session Service statistics
    Total packets            :0
    Message packets          :0
    Request packets          :0
    Positive response packets:0
    Negative response packets:0
    Retarget response packets:0
    Keepalive packets        :0
    Unknown packets          :0
    Total error packets      :0
```

Table 170 describes the significant fields shown in the display.

Table 170 show platform hardware qfp feature Field Descriptions

Field	Description
No. of allocated chunk elements in L7 data pool	Number of memory chunks allocated for processing NetBIOS packets.
No. of times L7 data is allocated:0 No. of times L7 data is freed	Number of times memory is allocated and freed for processing NetBIOS packets.
Direct unique packets	Number of direct unique NetBIOS packets processed.
Direct group packets	Number of direct group NetBIOS packets processed.
Broadcast packets	Number of broadcast NetBIOS packets processed.
DGM Error packets	Number of Datagram Error NetBIOS packets processed.
Query request packets	Number of query request NetBIOS packets processed.
Positive Qry response packets	Number of positive query response NetBIOS packets processed.
Negative Qry response packets	Number of negative query response NetBIOS packets processed.
Unknown packets	Number of unknown packets.
Total error packets	Counter tracking number of error packets.

The following example displays SIP statistics information of the processor. The field descriptions are self-explanatory.

```
Router# show platform hardware qfp active feature alg statistics sip

SIP info pool used chunk entries number: 0

RECEIVE
Register: 0 -> 200-OK: 0
Invite: 0 -> 200-OK: 0 Re-invite 0
Update: 0 -> 200-OK: 0
Bye: 0 -> 200-OK: 0
Trying: 0 Ringing: 0 Ack: 0
Info: 0 Cancel: 0 Sess Prog: 0
Message: 0 Notify: 0 Prack: 0
OtherReq: 0 OtherOk: 0
Events
Null dport: 0 Media Port Zero: 0
Malform Media: 0 No Content Length: 0
Cr Trunk Chnls: 0 Del Trunk Chnls: 0
Cr Normal Chnls: 0 Del Normal Chnls: 0
Media Addr Zero: 0 Need More Data: 0
Errors
Create Token Err: 0 Add portlist Err: 0
Invalid Offset: 0 Invalid Pktlen: 0
Free Magic: 0 Double Free: 0
Retmem Failed: 0 Malloc Failed: 0
Bad Format: 0 Invalid Proto: 0
Add ALG state Fail: 0 No Call-id: 0
Parse SIP Hdr Fail: 0 Parse SDP Fail: 0
Error New Chnl: 0 Huge Size: 0
Create Failed: 0
```

```
Writeback Errors
Offset Err: 0 PA Err: 0
No Info: 0
```

Related Commands

Command	Description
debug platform hardware qfp feature	Debugs feature-specific information in the QFP.

show platform hardware qfp act feature ipsec datapath memory

To display debugging information about the consumption of IPsec datapath memory, use the **show platform hardware qfp act feature ipsec datapath memory** command in privileged EXEC or diagnostic mode.

show platform hardware qfp act feature ipsec datapath memory

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Diagnostic (diag)

Command History

Release	Modification
Cisco IOS XE Release 2.4.2	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

This command displays the consumption of dynamic random access memory (DRAM) on the IPSec Cisco QuantumFlow Processor (QFP) datapath.

```
show platform hardware qfp act feature ipsec datapath memory

pstate chunk totalfree: 80000, allocated: 0
```

Related Commands

Command	Description
show platform software ipsec f0 encryption-processor registers	Displays dubugging information about the crypto engine processor registers.

show platform software ipsec f0 encryption-processor registers

To display debugging information about the crypto engine processor registers, use the **show platform software ipsec f0 encryption-processor registers** command in privileged EXEC or diagnostic mode.

show platform software ipsec f0 encryption-processor registers

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Diagnostic (diag)

Command History

Release	Modification
Cisco IOS XE Release 2.4.2	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

This command displays debugging information for crypto engine processor registers.

```
show platform software ipsec f0 encryption-processor registers

Forwarding Manager Encryption-processor Registers


     reg_addr : 00000000,    reg_val  : 0000ca5b
     reg_addr : 00000008,    reg_val  : 00000000
     reg_addr : 00000010,    reg_val  : 00000000
     reg_addr : 00000018,    reg_val  : 22f10038
     reg_addr : 00000020,    reg_val  : 00000800
     reg_addr : 00000028,    reg_val  : 00002040
     reg_addr : 00000030,    reg_val  : 00000000
     reg_addr : 00000038,    reg_val  : 23158838
```

Related Commands

Command	Description
show platform hardware qfp act feature ipsec datapath memory	Displays debugging information about the consumption of IPsec datapath memory.

show policy-firewall config

To display the firewall configuration on the router, use the **show policy-firewall config** command in privileged EXEC mode.

show policy-firewall config {**all** | **class-map** [*class-map-name* | *protocol-name*] | **parameter-map** [*parameter-map-name* | **default** | **global** | **protocol-info** | **regex** [*protocol-info-name*]] | **policy-map** [*policy-map-name* | *protocol-name*] | **zone** [**self**] | **zone-pair**}

Syntax Description

all	Displays the entire firewall configuration on the router.
class-map *class-map-name*	Displays the class-maps configured on the router.
protocol-name	Displays the protocols configured for the class-map.
parameter-map	Displays the parameter-maps configured in the router.
parameter-map-name	Displays configuration information about a specific parameter map.
default	Displays configuration information about the default inspect parameter map.
global	Displays configuration information about the global inspect parameter map.
protocol-info	Displays configuration information about the protocol-specific inspect parameter map.
regex	Displays configuration information about the regex inspect parameter map.
protocol-info-name	Displays configuration information about a specific protocol.
policy-map *policy-map-name*	Displays the policy maps configured on the router.
protocol-name	Displays the protocols configured for the policy map.
zone	Displays configuration information about the zones configured on the router.
self	(Optional) Displays configuration information about the system-defined zone.
zone-pair	Displays configuration information about each each zone-pair.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

Use this command to display a summary of the firewall configuration on the router.

Examples

The following is the sample output from the **show policy-firewall config all** command. The field descriptions are self-explanatory.

```
Router# show policy-firewall config all
Zone: self
  Description: System defined zone
```

```
Parameter-map Config:
 Global:
  alert on
  sessions maximum 2147483647
  waas disabled
  l2-transparent dhcp-passthrough disabled
  dropped-packets disabled
  log summary disabled
  max-incomplete low 2147483647
  max-incomplete high 2147483647
  one-minute low 2147483647
  one-minute high 2147483647
 Default:
  audit-trail off
  alert on
  max-incomplete low 2147483647
  max-incomplete high 2147483647
  one-minute low 2147483647
  one-minute high 2147483647
  udp idle-time 30
  icmp idle-time 10
  dns-timeout 5
  tcp idle-time 3600
  tcp finwait-time 5
  tcp synwait-time 30
  tcp max-incomplete host 4294967295 block-time 0
  sessions maximum 2147483647
```

The following example is a sample output from the **show policy-firewall config class-map** command:

```
Router# show policy-firewall config class-map c1
Class Map type inspect match-all c1 (id 1)
   Match access-group  101
   Match protocol http
```

The following example shows output related to user-defined parameter map:

```
Router# show policy-firewall config parameter-map params1
parameter-map type inspect params1
  audit-trail off
  alert on
  max-incomplete low 2147483647
  max-incomplete high 2147483647
  one-minute low 2147483647
  one-minute high 2147483647
  udp idle-time 30
  icmp idle-time 10
  dns-timeout 5
  tcp idle-time 3600
  tcp finwait-time 5
  tcp synwait-time 30
  tcp max-incomplete host 4294967295 block-time 0
  sessions maximum 2147483647
```

The following example shows output related default parameter map:

```
Router# show policy-firewall config parameter-map default
  audit-trail off
  alert on
  max-incomplete low 2147483647
  max-incomplete high 2147483647
  one-minute low 2147483647
  one-minute high 2147483647
  udp idle-time 30
```

```
  icmp idle-time 10
  dns-timeout 5
  tcp idle-time 3600
  tcp finwait-time 5
  tcp synwait-time 30
  tcp max-incomplete host 4294967295 block-time 0
  sessions maximum 2147483647
```

The following example shows output related to global parameter map:

```
Router# show policy-firewall config parameter-map global

  alert on
  sessions maximum 2147483647
  waas disabled
  l2-transparent dhcp-passthrough disabled
  log dropped-packets disabled
  log summary disabled
  max-incomplete low 2147483647
  max-incomplete high 2147483647
  one-minute low 2147483647
  one-minute high 2147483647
```

show policy-firewall mib

To display connection statistics of the firewall policy on the router, use the **show policy-firewall mib** command in privileged EXEC mode.

show policy-firewall mib connection-statistics {**global** | **policy** *policy-name* **zone-pair** *name* | **L4-Protocol** | **L7-Protocol** |}{*name* | **all**}

Syntax Description

connection-statistics	Displays the statistics for one of the following selected options.
global	Displays the global connection statistics.
policy *policy-name*	Displays statistics for a specific firewall policy.
zone-pair *name*	Displays statistics for a zone pair in a specific firewall policy.
L4-Protocol *name*	Displays statistics for a specific Layer 4 protocol.
L7-Protocol *name*	Displays statistics for a specific Layer 7 protocol.
all	Displays statistics for all Layer 4 or Layer 7 protocols.

Command Default

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

Use this command to display the global connection statistics and the statistics per protocol in Layer 4 or Layer 7 for each policy or zone pair. Use the **debug policy-firewall mib** command to toggle on or off the support for MIBs in zone-based policy firewalls.

Examples

The following is sample output from five versios of the **show policy-firewall mib** command:

```
Router# show policy-firewall mib connection-statistics global
-------------------------------------------------
Connections Attempted                           26
Connections Setup Aborted                       0
Connections Policy Declined                     0
Connections Resource Declined                   0
Connections Half Open                           0
Connections Active                              0
Connections Expired                             25
Connections Aborted                             0
Connections Embryonic                           0
Connections 1-min Setup Count                   0
Connections 5-min Setup Count                   0

Router# show policy-firewall mib connection-statistics L4-Protocol all
-------------------------------------------------
Protocol                                      udp
Connections Attempted                           1
Connections Setup Aborted                       0
Connections Policy Declined                     0
```

```
Connections Resource Declined                    0
Connections Half Open                            0
Connections Active                               0
Connections Aborted                              0
Connections Embryonic                            0
Connections 1-min Setup Count                    0
Connections 5-min Setup Count                    0
-------------------------------------------------
Protocol                                    tcp
Connections Attempted                            25
Connections Setup Aborted                        0
Connections Policy Declined                      0
Connections Resource Declined                    0
Connections Half Open                            0
Connections Active                               0
Connections Aborted                              0
Connections Embryonic                            0
Connections 1-min Setup Count                    0
Connections 5-min Setup Count                    0

Router# show policy-firewall mib connection-statistics L7-Protocol all
-------------------------------------------------
Protocol                                    http
Connections Attempted                            14
Connections Setup Aborted                        0
Connections Policy Declined                      0
Connections Resource Declined                    0
Connections Half Open                            0
Connections Active                               0
Connections Aborted                              0
Connections Embryonic                            0
Connections 1-min Setup Count                    0
Connections 5-min Setup Count                    0
-------------------------------------------------
Protocol                                    tacacs
Connections Attempted                            12
Connections Setup Aborted                        0
Connections Policy Declined                      0
Connections Resource Declined                    0
Connections Half Open                            0
Connections Active                               0
Connections Aborted                              0
Connections Embryonic                            0
Connections 1-min Setup Count                    0
Connections 5-min Setup Count                    0

Router# show policy-firewall mib connection-statistics policy inout-policy zone-pair inout
L4-Protocol all
-------------------------------------------------
Policy                                      inout-policy
Zone-pair                                   inout
-------------------------------------------------
Protocol                                    udp
Connections Attempted                            1
Connections Setup Aborted                        0
Connections Policy Declined                      0
Connections Resource Declined                    0
Connections Half Open                            0
Connections Active                               0
Connections Aborted                              0
-------------------------------------------------
Protocol                                    tcp
Connections Attempted                            11
Connections Setup Aborted                        0
```

```
Connections Policy Declined                          0
Connections Resource Declined                        0
Connections Half Open                                0
Connections Active                                   0
Connections Aborted                                  0

Router# show policy-firewall mib connection-statistics policy inout-policy zone-pair inout
L7-Protocol all
-------------------------------------------------
Policy                                          inout-policy
Zone-pair                                       inout
-------------------------------------------------
Protocol                                        tacacs
Connections Attempted                                12
Connections Setup Aborted                            0
Connections Policy Declined                          0
Connections Resource Declined                        0
Connections Half Open                                0
Connections Active                                   0
Connections Aborted                                  0
```

Table 171 describes the significant fields shown in the displays.

Table 171 show policy-firewall mib Field Descriptions

Field	Description
Connections Attempted	The total number of connection attempts sent to the firewall. This is a cumulative value.
Connections Policy Declined	The number of connection attempts that were declined due to a firewall security policy. This is a cumulative value.
Connections Resource Declined	The number of connection attempts that were declined due to firewall resource constraints. This is a cumulative value.
Connections Half Open	The number of connections that are being established with the firewall. This is a reflection of the current state of the system.
Connections Active	The number of connections that are currently active. This is a reflection of the current state of the system.
Connections Expired	The number of connections that were active and terminated. This is a cumulative value.
Connections Aborted	The number of connections that were abnormally terminated after a successful connection. This is a cumulative value.
Connections Embryonic	The number of embryonic application layer connections. This is a reflection of the current state of the system.
Connections 1-min Setup Count	The number of connections that the firewall attempts to establish per second averaged over the last 60 seconds. This is a reflection of the current state of the system.
Connections 5-min Setup Count	The number of connections that the firewall attempts to establish per second, averaged over the last 300 seconds. This is a reflection of the current state of the system.

Related Commands

Command	Description
debug policy-firewall mib	Toggles on or off the MIB support.

show policy-firewall session

To display the session details of a firewall policy, use the **show policy-firewall session** command in privileged EXEC mode.

show policy-firewall session [**msrpc** | **zone-pair**]

Syntax Description

msrpc	(Optional) Displays the Microsoft Remote Procedure Call (MSRPC) sessions.
zone-pair	(Optional) Displays the sessions pertaining to the zone pairs.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. The **msrpc** keyword was added.

Usage Guidelines

Use the **show policy-firewall session** command to display the session details. Sessions details could either be global, zone pair-specific or MSRPC-specific. Global session details incorporate all the sessions created by the firewall, and zone pair-specific details pertain to each zone pair.

Examples

The following is sample output from the **show policy-firewall session** command:

```
Router# show policy-firewall session zone-pair

Zone-pair: zone-pair-source2destination

  Service-policy inspect : policy-test

    Class-map: class-test (match-any)
   Inspect

      Number of Established Sessions = 100
      Established Sessions
        Session 3F4DF38 (10.0.0.148:13686)=>(11.0.0.33:80) http:tcp SIS_OPEN
          Created 00:00:02, Last heard 00:00:01
          Bytes sent (initiator:responder) [257:10494]
        Session 43F0F58 (10.0.0.149:13687)=>(11.0.0.33:80) http:tcp SIS_OPEN
          Created 00:00:02, Last heard 00:00:01
          Bytes sent (initiator:responder) [274:10494]
        Session 3F3BD98 (10.0.0.98:13770)=>(11.0.0.33:80) http:tcp SIS_OPEN
          Created 00:00:02, Last heard 00:00:02
          Bytes sent (initiator:responder) [251:0]
        Session 3F2E498 (10.0.0.104:13774)=>(11.0.0.33:80) http:tcp SIS_OPEN
          Created 00:00:02, Last heard 00:00:01
          Bytes sent (initiator:responder) [277:10220]
        Session 3F3B008 (10.0.0.105:13775)=>(11.0.0.33:80) http:tcp SIS_OPEN
          Created 00:00:02, Last heard 00:00:01
          Bytes sent (initiator:responder) [264:10220]
```

```
    Session 3F31AD8 (10.0.0.108:13776)=>(11.0.0.33:80) http:tcp SIS_OPEN
      Created 00:00:02, Last heard 00:00:01
      Bytes sent (initiator:responder) [265:10220]
    Session 2F91030 (10.0.0.113:13780)=>(11.0.0.33:80) http:tcp SIS_OPEN
      Created 00:00:02, Last heard 00:00:01
      Bytes sent (initiator:responder) [257:10220]
    Session 3F35308 (10.0.0.229:13966)=>(11.0.0.33:80) http:tcp SIS_OPEN
      Created 00:00:00, Last heard 00:00:00
      Bytes sent (initiator:responder) [278:10494]
    Session 3F30B58 (10.0.0.231:13968)=>(11.0.0.33:80) http:tcp SIS_OPEN
      Created 00:00:00, Last heard 00:00:00
      Bytes sent (initiator:responder) [257:10494]
    Session 3F30588 (10.0.0.234:13969)=>(11.0.0.33:80) http:tcp SIS_OPEN
      Created 00:00:00, Last heard 00:00:00
      Bytes sent (initiator:responder) [259:10494]

  Number of Half-open Sessions = 8
  Half-open Sessions
    Session 3F32298 (10.0.0.99:13068)=>(11.0.0.33:80) http:tcp SIS_OPENING
      Created 00:00:06, Last heard 00:00:06
      Bytes sent (initiator:responder) [0:0]
    Session 2F8F510 (10.0.0.123:13428)=>(11.0.0.33:80) http:tcp SIS_OPENING
      Created 00:00:04, Last heard 00:00:04
      Bytes sent (initiator:responder) [0:0]
    Session 3F4E128 (10.0.0.125:13430)=>(11.0.0.33:80) http:tcp SIS_OPENING
      Created 00:00:04, Last heard 00:00:04
      Bytes sent (initiator:responder) [0:0]
    Session 3F4E318 (10.0.0.126:13431)=>(11.0.0.33:80) http:tcp SIS_OPENING
      Created 00:00:04, Last heard 00:00:04
      Bytes sent (initiator:responder) [0:0]
    Session 3F4E6F8 (10.0.0.127:13432)=>(11.0.0.33:80) http:tcp SIS_OPENING
      Created 00:00:04, Last heard 00:00:04
      Bytes sent (initiator:responder) [0:0]
    Session 43ECF68 (10.0.0.138:13561)=>(11.0.0.33:80) http:tcp SIS_OPENING
      Created 00:00:03, Last heard 00:00:03
      Bytes sent (initiator:responder) [0:0]
    Session 3F4D968 (10.0.0.130:13674)=>(11.0.0.33:80) http:tcp SIS_OPENING
      Created 00:00:02, Last heard 00:00:02
      Bytes sent (initiator:responder) [0:0]
    Session 3F4DB58 (10.0.0.147:13685)=>(11.0.0.33:80) http:tcp SIS_OPENING
      Created 00:00:02, Last heard 00:00:02
      Bytes sent (initiator:responder) [0:0]

  Number of Terminating Sessions = 3
  Terminating Sessions
    Session 2F9DD90 (10.0.0.203:13603)=>(11.0.0.33:80) http:tcp SIS_CLOSING
      Created 00:00:03, Last heard 00:00:02
      Bytes sent (initiator:responder) [268:10494]
    Session 3F3AA38 (10.0.0.209:13844)=>(11.0.0.33:80) http:tcp SIS_CLOSING
      Created 00:00:01, Last heard 00:00:01
      Bytes sent (initiator:responder) [251:2301]
    Session 43F20C8 (10.0.0.224:14070)=>(11.0.0.33:80) http:tcp SIS_CLOSING
      Created 00:00:00, Last heard 00:00:00
      Bytes sent (initiator:responder) [264:2301]

Zone-pair: zone-pair-destination2source
  Service-policy inspect : policy-test
    Class-map: class-test (match-any)
   Inspect
```

Table 172 describes the significant fields shown in the display.

Table 172 show policy-firewall session Field Descriptions

Field	Description
Number of Established Sessions	Number of established sessions. A session is established when the traffic flows between the sessions.
Number of Half-open Sessions	Number of half-open sessions. A TCP session that has not yet reached the established state is called a half-opened session.
Number of Terminating Sessions	A link or session between a pair of devices that get closed. The terminating side waits for a timeout and closes the connection between the devices; at this point of time, the local port of the terminating side is not available for new connections.

show policy-firewall stats

To display the statistics of the firewall activity on the router, use the **show policy-firewall stats** command in privileged EXEC mode.

show policy-firewall stats [**all** | **drop-counters** | **zone-pair** [**name**]]

Syntax Description

all	(Optional) Displays all firewall statistics on the router.
drop-counters	(Optional) Displays the number of packets dropped for each error code.
zone-pair *name*	(Optional) Displays statistics pertaining to zone-pair.

Command Default

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command provides the statistics of all the firewall activity on the router. The command displays the box-wide statistics or the statistics for each zone pair. To get all statistics, use the **all** keyword. Use the **drop-counters** keyword to display the packets dropped and grouped by their error codes. The output displays only the error codes for which the drop counter is greater than zero. If the number of packets dropped is similar for multiple error codes, the error codes are sorted in alphabetical order.

Examples

The following is sample output from the **show policy-firewall stats** command. The field descriptions are self-explanatory.

```
Router# show policy-firewall stats drop-counters
REASON                                          PACKETS DROPPED
    Invalid Header length                          39
    policy match failure                           38
    Police rate limiting                           37
    Session limiting                               36
    Bidirectional traffic disabled                 35
    SYN with data or with PSH/URG flags            34
    Segment matching no TCP connection             33
    Invalid Segment                                32
    Invalid Seq#                                   31
    Invalid Ack (or no Ack)                        30
    Invalid Flags                                  29
    Invalid Checksum                               28
    SYN inside current window                      27
    RST inside current window                      26
    Out-Of-Order Segment                           25
    Retransmitted Segment                          24
    Retransmitted Segment with Invalid Flags       23
    Stray Segment                                  22
    Internal Error                                 21
    Invalid Window scale option                    20
    Invalid TCP options                            19
```

```
No zone-pair between zones                        18
One of the interfaces not being configured for zoning 17
Policy not present on zone-pair                   16
DROP action found in policy-map                   15
```

show policy-firewall stats vrf

To display VPN Routing and Forwarding (VRF)-level policy firewall statistics, use the **show policy-firewall stats** command in user EXEC or privileged EXEC mode.

show policy-firewall stats vrf [*vrf-name*]

Syntax Description

vrf-name	(Optional) VRF name.

Command Default

This command has no default settings.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Examples

The following is sample output from the **show policy-firewall stats vrf** command:

```
Router# show policy-firewall stats vrf vpmap1

  VRF: vrf1, Parameter-Map: vpmap1
  Interface reference count: 0
       total_session_cnt: 0
       exceed_cnt:        0
       tcp_half_open_cnt: 0
       syn_exceed_cnt:    0
```

Table 173 describes the significant fields shown in the display.

Table 173 show policy-firewall stats vrf Field Descriptions

Field	Description
total_session_cnt	Total session count.
exceed_cnt	Number of sessions that exceeded the configured session count.
tcp_half_open_cnt	TCP half-open sessions configured for each VRF. When the configured session limit is reached, the TCP SYN cookie verifies the source of the half-open TCP sessions before creating more sessions. A TCP half-open session is a session that has not reached the established state.
syn_exceed_count	Number of synchronization (SYN) packets that exceeded the configured SYN flood rate limit.

Related Commands

Command	Description
clear policy-firewall stats vrf	Clears the policy firewall statistics counter at a VRF level.

show policy-firewall stats vrf global

To display global VPN Routing and Forwarding (VRF) firewall policy statistics, use the **show policy-firewall stats vrf global** command in user EXEC or privileged EXEC mode.

show policy-firewall stats vrf global

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Examples

The following is sample output from the **show policy-firewall stats vrf global** command:

```
Router# show policy-firewall stats vrf global

Global table statistics
       total_session_cnt: 0
       exceed_cnt:        0
       tcp_half_open_cnt: 0
       syn_exceed_cnt:    0
```

Table 174 describes the fields shown in the display.

Table 174 show policy-firewall stats vrf global Field Descriptions

Field	Description
total_session_cnt	Total session count.
exceed_cnt	Number of sessions that exceeded the configured session count.
tcp_half_open_cnt	TCP half-open sessions configured at a global VRF level. When the configured session limit is reached, the TCP synchronization (SYN) cookie verifies the source of the half-open TCP sessions before creating more sessions. A TCP half-open session is a session that has not reached the established state.
syn_exceed_cnt	Number of SYN packets that exceeded the configured SYN flood rate limit.

Related Commands

Command	Description
clear policy-firewall stats vrf global	Clears the global VRF policy firewall statistics.

show policy-firewall stats zone

To display policy firewall statistics at a zone level, use the **show policy-firewall stats zone** command in user EXEC or privileged EXEC mode.

show policy-firewall stats zone [*zone-name*]

Syntax Description

zone-name	(Optional) Zone name.

Command Default

This command has no default settings.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Examples

The following is sample output from the **show policy-firewall stats zone** command:

```
Router# show policy-firewall stats zone zone02

Zone: zone02
Parameter-map: zpmap01
TCP SYN packet conform limit: 10
TCP SYN packet exceed limit: 4
```

Table 175 describes the fields shown in the display.

Table 175 show policy-firewall stats zone Field Descriptions

Field	Description
Zone	Name of the zone.
Parameter-map	Name of the configured zone-type parameter map.
TCP SYN packet conform limit	Number of TCP synchronization (SYN) packets that are within the configured limit.
TCP SYN packet exceed limit	Number of TCP synchronization (SYN) packets that exceeded the configured SYN packet rate limit.

Related Commands

Command	Description
clear policy-firewall stats zone	Clears the policy firewall statistics counter at a zone level.
tcp syn-flood limit	Configures a limit to the number of TCP half-open sessions before triggering SYN cookie processing for new SYN packets.

show policy-firewall summary-log

To display summary logs, use the **show policy-firewall summary log** command in privileged EXEC mode.

show policy-firewall summary-log

Syntax Description

This command has no arguments or keywords.

Command Default

Summary logs are not displayed.

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

Use this command to display the summary logs captured as follows:

- Configured flow
- Configured flow value
- Number of flows

Note When the number of flows for the log summary reaches the configured flow value, some flows are not summarized.

Examples

The following is sample output from the **show policy-firewall summary-log**. The field descriptions are self-explanatory.

```
Router# show policy-firewall summary-log

*Apr 1 12:38:29.103: %FW-6-LOG_SUMMARY: 10 http packets were dropped from
10.0.0.1:1024 => 20.0.0.1:23 (target: class)-(z1toz2:C1)
```

Related Commands

Command	Description
clear policy-firewall	Clears the information collected by the firewall.

show policy-map type inspect

To display a specified policy map, use the **show policy-map type inspect** command in privileged EXEC mode.

show policy-map type inspect [*policy-map-name*] [**class** *class-map-name*]

Syntax Description

policy-map-name	(Optional) Name of the policy map.
class *class-map-name*	(Optional) Name of the class map.

Command Default

If a policy-map name is not specified, all Level 7 policy maps are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Examples

The following example displays the policy map for policy map p1:

```
Router # show policy-map type inspect p1

 Policy Map type inspect p1
  Class c1
   Inspect
```

The following example shows sample command output:

```
Router# show policy-map type inspect p_inside

Policy Map type inspect p_inside
 Description: Policy map with inspect action
 Class c_permit
  Pass
 Class c_test
 Class class-default
```

Table 176 describes the significant fields shown in the display.

Table 176 show policy-map type inspect Field Descriptions

Field	Description
p_inside	Name of the policy map.
Description	Description of the policy map.

Table 176 show policy-map type inspect Field Descriptions (continued)

Field	Description
Class	Name of the class map.
Pass	Allows packets to be sent to the router without being inspected.

show policy-map type inspect urlfilter

To display the details of a URL filtering policy map, use the **show policy-map type inspect urlfilter** command in privileged EXEC mode.

show policy-map type inspect urlfilter [*policy-map-name*]

Syntax Description

policy-map-name	(Optional) Name of the policy map for which details are displayed.

Command Default

The details of all URL filtering policy maps are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **show policy-map type inspect urlfilter** command to display the details of all URL filtering policy maps. To display the details of a particular URL filtering policy map, specify the name of the policy map.

Examples

The following is sample output from the **show policy-map type inspect urlfilter** command for a policy map named websense-policy:

```
Router# show policy-map type inspect urlfilter websense-policy

policy-map type inspect urlfilter url-websense-policy
  parameter-map urlfpolicy websense websense-parameter-map
  class type urlfilter trusted-domain-lists
   allow
  class type urlfilter untrusted-domain-lists
   reset
  class type urlfilter block-url-keyword-lists
   reset
  class type urlfilter websense websense-map
   server-specified-action
```

show policy-map type inspect zone-pair

To display the runtime inspect type policy map statistics and other information such as sessions existing on a specified zone pair, use the **show policy-map type inspect zone-pair** command in privileged EXEC mode.

show policy-map type inspect zone-pair [*zone-pair-name*] [sessions]

Syntax Description

zone-pair-name	(Optional) Zone pair for which the system displays the runtime inspect type policy-map statistics. Default: The requested information is shown for all zone pairs.
sessions	(Optional) Displays the Cisco IOS stateful packet inspection sessions created because of the policy-map application on the specified zone pair.

Command Default

If the optional argument and keyword are not entered, information about policy maps for all zone pairs is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(9)T	The output from this command was enhanced to display the police action configuration.
12.4(15)XZ	This command was implemented on the following platforms: Cisco 881 and Cisco 888.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

If you do not specify a zone-pair name, the policy maps on all zone pairs are displayed.

When packets are matched to an access group (**match access-group**), protocol (**match protocol**), or class map (**match class-map**), a traffic rate is generated for these packets. In a zone-based firewall policy, only the first packet that creates a session matches the policy. Subsequent packets in this flow do not match the filters in the configured policy, but instead match the session directly. The statistics related to subsequent packets are shown as part of the “inspect” action. This information is shown when using the **show policy-map type inspect zone-pair sessions** command.

Command Limitations

The cumulative counters in the **show policy-map type inspect zone-pair** command output do not increment for **match** statements in a nested class-map configuration in Cisco IOS Releases 12.4(20)T and 12.4(15)T. The problem with the counters exists regardless of whether the top level class map uses the **match-any** or **match-all** keywords.

The following configuration example causes the match counter problem in the **show policy-map type inspect zone-pair** command output:

```
class-map type inspect match-any y
 match protocol tcp
 match protocol icmp
class-map type inspect match-all x
 match class y
```

However, cumulative counters for the above configuration are displayed in the **show policy-map type inspect zone-pair** command output if the class map matches any class map:

```
Router# show policy-map type inspect zone-pair session

policy exists on zp zp
 Zone-pair: zp

  Service-policy inspect : fw

    Class-map: x (match-any)
      Match: class-map match-any y
        2 packets, 48 bytes   <======== Cumulative class map counters are incrementing.
        30 second rate 0 bps
        Match: protocol tcp
          0 packets, 0 bytes     <===== The match for the protocol is not incrementing.
          30 second rate 0 bps
        Match: protocol icmp
          0 packets, 0 bytes
          30 second rate 0 bps

   Inspect

      Number of Established Sessions = 1
      Established Sessions
        Session 53105C0 (1.1.1.2:19180)=>(2.1.1.2:23) tacacs:tcp SIS_OPEN
          Created 00:00:02, Last heard 00:00:02
          Bytes sent (initiator:responder) [30:69]

    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes
```

Examples

The following examples show sample output when a zone pair name is specified:

```
Router# show policy-map type inspect zone-pair zp

 Zone-pair: zp

  Service-policy : p1

   Class-map: c1 (match-all)
    Match: protocol tcp
    Inspect
     Session creations since subsystem startup or last reset 0
```

```
     Current session counts (estab/half-open/terminating) [0:0:0]
     Maxever session counts (estab/half-open/terminating) [0:0:0]
     Last session created never
     Last statistic reset never
     Last session creation rate 0
     half-open session total 0

   Class-map: c2 (match-all)
    Match: protocol udp
    Pass
     0 packets, 0 bytes

   Class-map: class-default (match-any)
    Match: any
    Drop
     0 packets, 0 bytes

Router# show policy-map type inspect zone-pair trusted_untrusted

 Zone-pair: trusted_untrusted
  Service-policy inspect : firewall_policy

Class-map: class_4 (match-any)
      Match: protocol dbcontrol_agent
      Match: protocol ddns-v3
      Match: protocol dhcp-failover
      Match: protocol discard
      Match: protocol dns
      Match: protocol dnsix
      Match: protocol echo
      Match: protocol entrust-svc-handler
      Inspect
        Packet inspection statistics [process switch:fast switch]
        dns packets: [0:28949015]
        Session creations since subsystem startup or last reset 4
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [1:0:0]
        Last session created 00:06:16
        Last statistic reset never
        Last session creation rate 0
        Last half-open session total 0
```

Note Only some important protocols may undergo the L7 inspections have the dedicated statistics and the others are grouped into either TCP statistics or UDP statistics.

The following example shows sample output when the **sessions** keyword is specified:

Note The information shown under the class-map field is the traffic rate (bits per second) of the traffic belonging to the connection initiating traffic only. Unless the connection setup rate is significantly high and sustained for multiple intervals over which the rate is computed, no significant data is shown for the connection.

```
Router# show policy-map type inspect zone-pair sessions

Zone-pair: hi2int

  Service-policy inspect : pg1
```

```
    Class-map: c1 (match-any)
      Match: protocol ftp
      Match: protocol telnet
      Match: protocol smtp
      Match: protocol http
      Match: protocol tacacs
      Match: protocol dns
      Match: protocol sql-net
      Match: protocol https
      Match: protocol tftp
      Match: protocol gopher
      Match: protocol finger
      Match: protocol kerberos
      Match: protocol pop3
      Match: protocol sunrpc
      Match: protocol msrpc
      Match: protocol icmp

      Inspect
        Established Sessions
         Session 10E28550 (10.1.1.1:50536)=>(172.16.1.1:111) sunrpc SIS_OPEN
          Created 00:09:44, Last heard 00:09:18
          Bytes sent (initiator:responder) [108:0]
         Session 10E28550 (10.1.1.1:39377)=>(172.16.1.1:150) sql-net SIS_CLOSED
          Created 00:03:01, Last heard 00:03:01
          Bytes sent (initiator:responder) [0:0]
         Session 10E2859C (10.1.1.1:39377)=>(172.16.1.1:110) pop3 SIS_CLOSED
          Created 00:02:59, Last heard 00:02:59
          Bytes sent (initiator:responder) [0:0]
         Session 10E285E8 (10.1.1.1:39377)=>(172.16.1.1:443) https SIS_CLOSED
          Created 00:03:33, Last heard 00:03:33
          Bytes sent (initiator:responder) [0:0]

    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        147127 packets, 8485742 bytes
```

The following example is sample output from the s**how policy-map type inspect zone-pair** command, which can now be used to verify the police action configuration:

```
Router# show policy-map type inspect zone-pair

Zone-pair: zp

Service-policy inspect : test-udp

  Class-map: check-udp (match-all)
   Match: protocol udp
   Inspect
    Packet inspection statistics [process switch:fast switch]
    udp packets: [3:4454]

    Session creations since subsystem startup or last reset 92
    Current session counts (estab/half-open/terminating) [5:33:0]
    Maxever session counts (estab/half-open/terminating) [5:59:0]
    Last session created 00:00:06
    Last statistic reset never
    Last session creation rate 61
    Last half-open session total 33
```

```
 Police
 rate 8000 bps,1000 limit
 conformed 2327 packets, 139620 bytes; actions: transmit
 exceeded 36601 packets, 2196060 bytes; actions: drop
 conformed 6000 bps, exceed 61000 bps

Class-map: class-default (match-any)
 Match: any
 Drop (default action)
 0 packets, 0 bytes
```

show policy-map type inspect zone-pair urlfilter

To display the details of a URL filtering policy map—URL filter state, URL filter statistics, and URL filter server details—use the **show policy-map type inspect zone-pair urlfilter** command in privileged EXEC mode.

show policy-map type inspect zone-pair [*zone-pair-name*] **urlfilter cache** [**detail**]

Syntax Description

zone-pair-name	(Optional) Zone pair for which the system will display the runtime inspect type policy-map statistics. Default: The requested information is shown for all zone pairs.
cache	Displays information about the URL filter cache.
detail	(Optional) Displays each entry in the cache. Because cache entries can be long, only the first few bytes are displayed.

Command Default

The URL filter information for all zone pairs is displayed. Details about the URL filtering cache are not displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was implemented on the following platforms: Cisco 881 and Cisco 888. The **detail** keyword was added to show more information about the URL filtering cache.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T. The **detail** keyword was added to show more information about the URL filtering cache.

Examples

The following example shows sample output for a Websense URL filtering server:

```
Router# show policy-map type inspect zone-pair urlfilter cache

Zone-pair: zp
 Urlfilter
 Websense URL Filtering is ENABLED

 Websense Primary server: 10.3.3.3(port : 15868)

 recount: 0
 Current packet buffer count(in use): 0
 Current cache entry count: 0

 Maxever request count: 0
 Maxever packet buffer count: 0
 Maxever cache entry count: 0

 Total requests sent to URL Filter Server :0
```

```
 Total responses received from URL Filter Server :0
 Total requests allowed: 0
 Total requests blocked: 0

Drop (default action)
 packets, 0 bytes

 Service-policy inspect : test

  Class-map: test (match-all)
   Match: protocol http

  Class-map: class-default (match-any)
   Match: any
```

The following example shows sample output for a Trend Micro URL filtering server, including the cache details:

```
Router# show policy-map type inspect zone-pair urlfilter cache detail

policy exists on zp zp_in
 Zone-pair: zp_in

 Service-policy inspect : trend-global-policy

  Class-map: http-class (match-all)
   Match: protocol http
   Match: access-group 101

 Inspect
   Packet inspection statistics [process switch:fast switch]
   tcp packets: [3353:0]

   Session creations since subsystem startup or last reset 21
   Current session counts (estab/half-open/terminating) [3:0:0]
   Maxever session counts (estab/half-open/terminating) [4:1:1]
   Last session created 00:00:22
   Last statistic reset never
   Last session creation rate 7
   Maxever session creation rate 14
   Last half-open session total 0
   Maximum number of bytes in cache: 131072000
   Time to live for eache cache entry (in hrs): 1
   Total number of bytes used by cache: 442
   Number of bytes used by domain type cache: 442
   Number of bytes used by directory type cache: 0
   ------------------------------------------------------------
   URL                                  Age   Access #/  Cat::Rep
   (Directory cache end with /)   (day:h:m:s)    Idle Time
   ------------------------------------------------------------
   example.com             0:00:00:23      28   58::100
   example1.com            0:00:00:25       1   56::100
   example.example2.com    0:00:00:34       1   56::100

  Class-map: class-default (match-any)
   Match: any
   Drop
     0 packets, 0 bytes

policy exists on zp zp_out
 Zone-pair: zp_out

 Service-policy inspect : icmp_permit
```

```
Class-map: icmp_permit (match-all)
 Match: access-group 110
 Pass
  0 packets, 0 bytes

Class-map: class-default (match-any)
 Match: any
 Drop
  0 packets, 0 bytes
```

show port-security

To display information about the port-security setting in EXEC command mode, use the **show port-security** command.

show port-security [**interface** *interface interface-number*]

show port-security [**interface** *interface interface-number*] {**address** | **vlan**}

Syntax Description

interface *interface*	(Optional) Specifies the interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, and **longreachethernet**.
interface-number	Interface number. Valid values are 1 to 6.
address	Displays all the secure MAC addresses that are configured on all the switch interfaces or on a specified interface with aging information for each address.
vlan	Virtual LAN.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	The **address** keyword was added to display the maximum number of MAC addresses configured per VLAN on a trunk port on the Supervisor Engine 720 only.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

The **vlan** keyword is supported on trunk ports only and displays per-Vlan maximums set on a trunk port.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

Examples

This example shows the output from the **show port-security** command when you do not enter any options:

```
Router# show port-security

Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security
Action
                    (Count)        (Count)      (Count)
-------------------------------------------------------------------------------

     Fa5/1           11            11            0            Shutdown
     Fa5/5           15            5             0            Restrict
     Fa5/11          5             4             0            Protect
-------------------------------------------------------------------------------

Total Addresses in System: 21
Max Addresses limit in System: 128
Router#
```

This example shows how to display port-security information for a specified interface:

```
Router# show port-security interface fastethernet 5/1

Port Security: Enabled
Port status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses: 11
Total MAC Addresses: 11
Configured MAC Addresses: 3
Aging time: 20 mins
Aging type: Inactivity
SecureStatic address aging: Enabled
Security Violation count: 0
Router#
```

This example show how to display all the secure MAC addresses that are configured on all the switch interfaces or on a specified interface with aging information for each address:

```
Router# show port-security address

Default maximum: 10
VLAN Maximum Current
1    5       3
2    4       4
3    6       4
Router#
```

Related Commands

Command	Description
clear port-security	Deletes configured secure MAC addresses and sticky MAC addresses from the MAC address table.

show ppp queues

To monitor the number of requests processed by each authentication, authorization, and accounting (AAA) background process, use the **show ppp queues** command in privileged EXEC mode.

show ppp queues

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show ppp queues** command to display the number of requests handled by each AAA background process, the average amount of time it takes to complete each request, and the requests still pending in the work queue. This information can help you balance the data load between the network access server and the AAA server.

This command displays information about the background processes configured by the **aaa processes** global configuration command. Each line in the display contains information about one of the background processes. If there are AAA requests in the queue when you enter this command, the requests will be printed as well as the background process data.

Examples

The following example shows output from the **show ppp queues** command:

```
Router# show ppp queues

Proc #0   pid=73  authens=59   avg. rtt=118s. authors=160  avg. rtt=94s.
Proc #1   pid=74  authens=52   avg. rtt=119s. authors=127  avg. rtt=115s.
Proc #2   pid=75  authens=69   avg. rtt=130s. authors=80   avg. rtt=122s.
Proc #3   pid=76  authens=44   avg. rtt=114s. authors=55   avg. rtt=106s.
Proc #4   pid=77  authens=70   avg. rtt=141s. authors=76   avg. rtt=118s.
Proc #5   pid=78  authens=64   avg. rtt=131s. authors=97   avg. rtt=113s.
Proc #6   pid=79  authens=56   avg. rtt=121s. authors=57   avg. rtt=117s.
Proc #7   pid=80  authens=43   avg. rtt=126s. authors=54   avg. rtt=105s.
Proc #8   pid=81  authens=139  avg. rtt=141s. authors=120  avg. rtt=122s.
Proc #9   pid=82  authens=63   avg. rtt=128s. authors=199  avg. rtt=80s.
queue len=0 max len=499
```

Table 177 describes the fields shown in the example.

Table 177 show ppp queues Field Descriptions

Field	Description
Proc #	Identifies the background process allocated by the **aaa processes** command to handle AAA requests for PPP. All of the data in this row relates to this process.
pid=	Identification number of the background process.
authens=	Number of authentication requests the process has performed.
avg. rtt=	Average delay (in seconds) until the authentication request was completed.
authors=	Number of authorization requests the process has performed.
avg. rtt=	Average delay (in seconds) until the authorization request was completed.
queue len=	Current queue length.
max len=	Maximum length the queue ever reached.

Related Commands

Command	Description
aaa processes	Allocates a specific number of background processes to be used to process AAA authentication and authorization requests for PPP.

show pppoe session

To display information about currently active PPP over Ethernet (PPPoE) sessions, use the **show pppoe session** command in privileged EXEC mode.

show pppoe session [**all** | **interface** *type number*] [**packets**]

Syntax Description

all	(Optional) Displays detailed information about the PPPoE session.
interface *type number*	(Optional) Displays information about the interface on which the PPPoE session is active.
packets	(Optional) Displays packet statistics for the PPPoE session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(4)YG	This command was introduced on the Cisco SOHO 76, 77, and 77H routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T and was enhanced to display information about relayed PPPoE Active Discovery (PAD) messages.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and support was added for the Cisco 7200, 7301, 7600, and 10000 series platforms.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2 and the output following the use of the **all** keyword was modified to indicate if a session is Interworking Functionality (IWF)-specific or if the **tag ppp-max-payload** tag is in the discovery frame and accepted.
12.4(15)XF	The output was modified to display Virtual Multipoint Interface (VMI) and PPPoE process-level values.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T to support VMIs in Mobile Ad Hoc Router-to-Radio Networks (MANETs).
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.

Examples

Single Session: Example

The following is sample output from the **show pppoe session** command:

```
Router# show pppoe session

     1 session  in FORWARDED (FWDED) State
     1 session  total
```

```
Uniq ID  PPPoE  RemMAC          Port     VT    VA      State    LocMAC           VA-st
         SID
26       19     0001.96da.a2c0  Et0/0.1  5     N/A     RELFWD   000c.8670.1006   VLAN:3434
```

PPPoE Session with IWF and ppp-max-payload Tag Example

The following is sample output from the **show pppoe session** command when there is an IWF session and the ppp-max-payload tag is accepted in the discovery frame (available in Cisco IOS Release 12.2(31)SB2):

```
Router# show pppoe session

     1 session  in LOCALLY_TERMINATED (PTA) State
     1 session  total.  1 session of it is IWF type

Uniq ID  PPPoE  RemMAC          Port    VT    VA      State    LocMAC           VA-st  Type
         SID
26       21     0001.c9f2.a81e  Et1/2   1     Vi2.1   PTA      0006.52a4.901e   UP     IWF
```

Table 178 describes the significant fields shown in the displays.

Table 178 show pppoe session Field Descriptions

Field	Description
Uniq ID	Unique identifier for the PPPoE session.
PPPoE SID	PPPoE session identifier.
RemMAC	Remote MAC address.
Port	Port type and number.
VT	Virtual-template interface.
VA	Virtual access interface.
State	Displays the state of the session, which will be one of the following: • FORWARDED • FORWARDING • LCP_NEGOTIATION • LOCALLY_TERMINATED • PPP_START • PTA • RELFWD (a PPPoE session was forwarded for which the Active discovery messages were relayed) • SHUTTING_DOWN • VACCESS_REQUESTED
LocMAC	Local MAC address.

show pppoe session all: Example

The following example shows information per session for the **show pppoe session all** command.

```
Router# show pppoe session all

Total PPPoE sessions 1


session id: 21
local MAC address: 0006.52a4.901e, remote MAC address: 0001.c9f2.a81e
virtual access interface: Vi2.1, outgoing interface: Et1/2, IWF
PPP-Max-Payload tag: 1500
    15942 packets sent, 15924 received
    224561 bytes sent, 222948 received
```

PPPoE Session Including Credit Flow Statistics Example

The following example shows the output from the **show pppoe session all** command. This version of the display includes PPPoE credit flow statistics for the session.

```
Router# show pppoe session all

Total PPPoE sessions 1
session id: 1
local MAC address: aabb.cc00.0100, remote MAC address: aabb.cc00.0200
virtual access interface: Vi2, outgoing interface: Et0/0
17 packets sent, 24 received
1459 bytes sent, 2561 received
PPPoE Flow Control Stats
Local Credits: 65504 Peer Credits: 65478
Credit Grant Threshold: 28000 Max Credits per grant: 65534
PADG Seq Num: 7 PADG Timer index: 0
PADG last rcvd Seq Num: 7
PADG last nonzero Seq Num: 0
PADG last nonzero rcvd amount: 0
PADG Timers: [0]-1000 [1]-2000 [2]-3000 [3]-4000
PADG xmit: 7 rcvd: 7
PADC xmit: 7 rcvd: 7
PADQ xmit: 0 rcvd: 0
```

Related Commands

Command	Description
clear pppoe relay context	Clears PPPoE relay contexts created for relaying PAD messages.
show pppoe relay context all	Displays PPPoE relay contexts created for relaying PAD messages.

show private-hosts access-lists

To display the access lists for your Private Hosts configuration, use the **show private-hosts access-lists** command in privileged EXEC mode.

show private-hosts access-lists

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following example shows how to display the Private Hosts access lists for your configuration:

```
Router# show private-hosts access-lists

Promiscuous ACLs
Action Permit   Sequence # 010
    Source:0000.1111.4001 0000.0000.0000 Destination:0000.0000.0000 ffff.ffff.ffff
Action Deny     Sequence # 020
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.0000.0000 ffff.ffff.ffff

Isolated ACLs
Action Deny     Sequence # 010
    Source:0000.1111.4001 0000.0000.0000 Destination:0000.0000.0000 ffff.ffff.ffff
Action Permit   Sequence # 020
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.1111.4001 0000.0000.0000 Action
Redirect Sequence # 030 Redirect index 6
    Source:0000.0000.0000 ffff.ffff.ffff Destination:ffff.ffff.ffff 0000.0000.0000
Action Permit   Sequence # 040
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0100.5e00.0000 0000.007f.ffff
    Source:0000.0000.0000 ffff.ffff.ffff Destination:3333.0000.0000 0000.ffff.ffff
Action Deny     Sequence # 050
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.0000.0000 ffff.ffff.ffff

Mixed ACLs
Action Permit   Sequence # 010
    Source:0000.1111.4001 0000.0000.0000 Destination:ffff.ffff.ffff 0000.0000.0000 Action
Redirect Sequence # 020 Redirect index 6
    Source:0000.0000.0000 ffff.ffff.ffff Destination:ffff.ffff.ffff 0000.0000.0000
Action Permit   Sequence # 030
    Source:0000.1111.4001 0000.0000.0000 Destination:0000.0000.0000 ffff.ffff.ffff
Action Permit   Sequence # 040
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.1111.4001 0000.0000.0000
Action Deny     Sequence # 050
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.0000.0000 ffff.ffff.ffff
```

Related Commands

Command	Description
show fm private-hosts	Displays information about the Private Hosts feature manager.
show private-hosts configuration	Displays Private Hosts configuration information for the networking device.
show private-hosts interface configuration	Displays Private Hosts configuration information for individual interfaces.

show private-hosts configuration

To display information about the Private Hosts configuration on the router, use the **show private-hosts configuration** command in privileged EXEC mode.

show private-hosts configuration

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following example shows sample command output:

```
Router# show private-hosts configuration

Private hosts enabled. BR INDEX 6 State 0000000F
Privated hosts vlans lists:
200
Privated promiscuous MAC configuration:
A '*' mark behind the mac list indicates non-existent mac-list
--------------------------------------------------------------------------------
MAC-list                      VLAN list
--------------------------------------------------------------------------------
bras-list                    *** Uses the isolated vlans (if any) ***
```

The following example shows sample command output:

```
Router# show private-hosts configuration

Private-hosts enabled
Isolated vlan-list 10,12,15,200-300
Promiscuous MAC configuration:
------------------------------------------------------------------------------------
MAC-List               VLAN List
-------------------------------------------------------------------------------
Bras_list              10,12,15,200-300
Mcast_server_list      10,12,15
Router#
```

Related Commands

Command	Description
private-hosts	Enables or configures the Private Hosts feature.
private-hosts mode	Sets the switchport mode.

Command	Description
show fm private-hosts interface configuration	Displays the FM-related Private Hosts information.
show private-hosts interface configuration	Displays Private Hosts configuration information for individual interfaces.

show private-hosts interface configuration

To display information about the Private Hosts configuration on individual interfaces (ports), use the **show private-hosts interface configuration** command in privileged EXEC mode.

show private-hosts interface configuration

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated in Cisco IOS Release 12.2(33)SXH.

Examples

The following example shows sample command output:

```
Router# show private-hosts interface configuration

Private hosts enabled
Debug Events: 0 Acl: 0 API: 0
Promiscuous interface list
--------------------------
GigabitEthernet1/1 promiscuous connected Facing BRAS Jupiter

Isolated interface list
-----------------------
FastEthernet3/1-14 isolated connected Facing DSLAM AB-125-1

Mixed mode interface list
-------------------------
GigabitEthernet1/4-5 mixed connected Facing Server Mars

Router#
```

Related Commands

Command	Description
private-hosts	Enables or configures the Private Hosts feature.
private-hosts mode	Sets the switchport mode.
show fm private-hosts	Displays the FM-related Private Hosts information.
show private-hosts configuration	Displays Private Hosts configuration information for the router.

show private-hosts mac-list

To display the contents of the MAC address lists defined for Private Hosts, use the **show private-hosts mac-list** command in privileged EXEC mode.

show private-hosts mac-list [*list-name*]

Syntax Description

list-name	(Optional) The name of the MAC address list whose contents you want to display.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following example shows sample command output:

```
Router# show private-hosts mac-list

MAC-List: bras-list
-----------------------------------------------------------------
MAC address    Description
-----------------------------------------------------------------
0000.1111.1111 BRAS-SERVER
```

Related Commands

Command	Description
private-hosts mac-list	Creates a MAC address list that identifies a content server that is being used to provide broadband services to isolated hosts.

show privilege

To display your current level of privilege, use the **show privilege** command in EXEC mode.

show privilege

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows sample output from the **show privilege** command. The current privilege level is 15.

```
Router# show privilege

Current privilege level is 15
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
enable secret	Specifies an additional layer of security over the **enable password** command.

show radius local-server statistics

To display the statistics for the local authentication server, use the **show radius local-server statistics** command in privileged EXEC mode.

show radius local-server statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)JA	This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Examples

The following output displays statistics for the local authentication server.

```
Router# show radius local-server statistics

Successes              : 11262       Unknown usernames      : 0
Client blocks          : 0           Invalid passwords      : 8
Unknown NAS            : 0           Invalid packet from NAS: 0

NAS : 10.0.0.1
Successes              : 11262       Unknown usernames      : 0
Client blocks          : 0           Invalid passwords      : 8
Corrupted packet       : 0           Unknown RADIUS message : 0
No username attribute  : 0           Missing auth attribute : 0
Shared key mismatch    : 0           Invalid state attribute: 0
Unknown EAP message    : 0           Unknown EAP auth type  : 0
PAC refresh            : 0           Invalid PAC received   : 0

Maximum number of configurable users: 50, current user count: 11
Username                   Successes  Failures  Blocks
vayu-ap-1                       2235         0       0
vayu-ap-2                       2235         0       0
vayu-ap-3                       2246         0       0
vayu-ap-4                       2247         0       0
vayu-ap-5                       2247         0       0
vayu-11                            3         0       0
vayu-12                            5         0       0
vayu-13                            5         0       0
vayu-14                           30         0       0
vayu-15                            3         0       0
scm-test                           1         8       0
```

The first section of statistics lists cumulative statistics from the local authenticator.

The second section lists statistics for each access point (NAS) authorized to use the local authenticator. The EAP-FAST statistics in this section include the following:

- Auto provision success—the number of PACs generated automatically
- Auto provision failure—the number of PACs not generated because of an invalid handshake packet or invalid username or password
- PAC refresh—the number of PACs renewed by clients
- Invalid PAC received—the number of PACs received that were expired, that the authenticator could not decrypt, or that were assigned to a client username not in the authenticator's database

The third section lists stats for individual users. If a user is blocked and the lockout time is set to infinite, *blocked* appears at the end of the stat line for that user. If the lockout time is not infinite, *Unblocked in x seconds* appears at the end of the stat line for that user.

Use the **clear radius local-server statistics** command in privileged EXEC mode to reset local authenticator statistics to zero.

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

show radius server-group

To display properties for the RADIUS server group, use the **show radius server-group** command in user EXEC or privileged EXEC mode.

show radius server-group {**server-group-name** | **all** | *123*}

Syntax Description

server-group-name	Displays properties for the server group named. The character string used to name the group of servers must be defined using the **aaa group server radius** command.
all	Displays properties for all the server group.
server	Displays properties for a specific server or servers in the group.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(33)SRA	The *server* argument was introduced.

Usage Guidelines

Use the **show radius server-group** command to display the server groups that you defined by using the **aaa group server radius** command.

Examples

The following **show radius server-group** command output displays properties for the server group "rad_sg":

```
Router# show radius server-group rad_sg

server group rad-sg
 Sharecount = 1  sg_unconfigured = FALSE
 Type = standard  Memlocks = 1
```

The following **show radius server-group** command output displays the properties for two server groups, 123 and 456, respectively. Using the **aaa group server radius** command, the configuration of each server group is also shown.

```
Router(config)# aaa new-model
!
!
Router(config)# aaa group server radius 123
 server 10.9.8.1 auth-port 1645 acct-port 1646
!
Router(config)# aaa group server radius 456
 server 10.9.8.2 auth-port 1645 acct-port 1646

Router(config)# exit

Router# show radius server-group all
```

```
Server group 123
 Sharecount = 1  sg_unconfigured = FALSE
 Type = standard

Server group 456
 Sharecount = 1  sg_unconfigured = FALSE
 Type = standard

Router# show radius server-group 123

Server group 123
 Sharecount = 1  sg_unconfigured = FALSE
 Type = standard
```

Table 179 describes the significant fields shown in the display.

Table 179 show radius server-group command Field Descriptions

Field	Description
Server group	Name of the server group.
Sharecount	Number of method lists that are sharing this server group. For example, if one method list uses a particular server group, the sharecount would be 1. If two method lists use the same server group, the sharecount would be 2.
sg_unconfigured	Server group has been unconfigured.
Type	The type can be either “standard” or “nonstandard”. The type indicates whether the servers in the group accept nonstandard attributes. If all servers within the group are configured with the nonstandard option, the type will be shown as “nonstandard”.
Memlocks	An internal reference count for the server-group structure that is in memory. The number represents how many internal data structure packets or transactions are holding references to this server group. Memlocks is used internally for memory management purposes.

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
show aaa servers	Displays information about the number of packets sent to and received from AAA servers.
show radius statistics	Displays the RADIUS statistics for accounting and authentication packets.

show radius statistics

To display the RADIUS statistics for accounting and authentication packets, use the **show radius statistics** command in EXEC mode.

show radius statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example is sample output for the **show radius statistics** command:

```
Router# show radius statistics
                                  Auth.       Acct.       Both
       Maximum inQ length:          NA          NA          1
       Maximum waitQ length:        NA          NA          2
       Maximum doneQ length:        NA          NA          1
       Total responses seen:        33          67        100
     Packets with responses:        33          67        100
  Packets without responses:         0           0          0
  Access Rejects           :         0
Average response delay(ms) :      1331         124        523
 Maximum response delay(ms):      5720        4800       5720
  Number of Radius timeouts:         8           2         10
       Duplicate ID detects:         0           0          0
 Buffer Allocation Failures:         0           0          0
Maximum Buffer Size (bytes):       156         327        327
Malformed Responses        :         0           0          0
Bad Authenticators         :         0           0          0
 Source Port Range: (2 ports only)
 1645 - 1646
 Last used Source Port/Identifier:
 1645/33
 1646/69
```

Table 180 describes significant fields shown in the display.

Table 180 show radius statistics Field Descriptions

Field	Description
Auth.	Statistics for authentication packets.
Acct.	Statistics for accounting packets.
Both	Combined statistics for authentication and accounting packets.
Maximum inQ length	Maximum number of entries allowed in the queue, that holds the RADIUS messages not yet sent.
Maximum waitQ length	Maximum number of entries allowed in the queue, that holds the RADIUS messages that have been sent and are waiting for a response.
Maximum doneQ length	Maximum number of entries allowed in the queue, that holds the messages that have received a response and will be forwarded to the code that is waiting for the messages.
Total responses seen	Number of RADIUS responses seen from the server. In addition to the expected packets, this includes repeated packets and packets that do not have a matching message in the waitQ.
Packets with responses	Number of packets that received a response from the RADIUS server.
Packets without responses	Number of packets that never received a response from any RADIUS server.
Access Rejects	Number of times access requests have been rejected by a radius server.
Average response delay	Average time from when the packet was first transmitted to when it received a response. If the response timed out and the packet was sent again, this value includes the timeout. If the packet never received a response, this is not included in the average.
Maximum response delay	Maximum delay observed while gathering average response delay information.
Number of RADIUS timeouts	Number of times a server did not respond, and the RADIUS server re-sent the packet.
Duplicate ID detects	RADIUS has a maximum of 255 unique IDs. In some instances there can be more than 255 outstanding packets. When a packet is received, the doneQ is searched from the oldest entry to the youngest. If the IDs are the same, further techniques are used to see if this response matches this entry. If it is determined that this does not match, the duplicate ID detect counter is increased.
Buffer Allocation Failures	Number of times the buffer failed to get allocated.

Table 180 show radius statistics Field Descriptions (continued)

Field	Description
Auth.	Statistics for authentication packets.
Acct.	Statistics for accounting packets.
Both	Combined statistics for authentication and accounting packets.
Maximum inQ length	Maximum number of entries allowed in the queue, that holds the RADIUS messages not yet sent.
Maximum Buffer Size (bytes)	Displays the maximum size of the buffer.
Malformed Responses	Number of corrupted responses, mostly due to bad authenticators.
Bad Authenticators	Number of authentication failures due to shared secret mismatches.
Source Port Range: (2 ports only)	Displays the port numbers.
Last used Source Port/Identifier	The ports that were last used by radius server for authentication.

Related Commands

Command	Description
radius-server host	Specifies a RADIUS server host.
radius-server retransmit	Specifies how many times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
radius-server timeout	Sets the interval for which a router waits for a server host to reply.

show radius table attributes

To display a list of all attributes supported by the RADIUS subsystem, use the **show radius table attributes** command in user EXEC or privileged EXEC mode.

show radius table attributes

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRA	This command was introduced.

Usage Guidelines

This command enables you to verify that a required RADIUS attribute is supported in a specific release.

Examples

The following example displays the complete table attribute list from the **show radius table attributes** command.

```
Router# show radius table attributes

IETF ATTRIBUTE LIST:
    Name User-Name                      Format String
    Name User-Password                  Format Binary
    Name CHAP-Password                  Format Binary
    Name NAS-IP-Address                 Format IPv4 Address
    Name NAS-Port                       Format Ulong
    Name Service-Type                   Format Enum
    Name Framed-Protocol                Format Enum
    Name Framed-IP-Address              Format IPv4 Address
    Name Framed-IP-Netmask              Format IPv4 Address
    Name Framed-Routing                 Format Ulong
    Name Filter-Id                      Format Binary
    Name Framed-MTU                     Format Ulong
    Name Framed-Compression             Format Enum
    Name login-ip-addr-host             Format IPv4 Address
    Name Login-Service                  Format Enum
    Name login-tcp-port                 Format Ulong
    Name Reply-Message                  Format Binary
    Name Callback-Number                Format String
    Name Framed-Route                   Format String
    Name Framed-IPX-Network             Format IPv4 Address
    Name State                          Format Binary
    Name Class                          Format Binary
    Name Vendor-Specific                Format Binary
    Name Session-Timeout                Format Ulong
    Name Idle-Timeout                   Format Ulong
    Name Termination-Action             Format Boolean
    Name Called-Station-Id              Format String
```

```
    Name Calling-Station-Id             Format String
    Name Nas-Identifier                 Format String
    Name Acct-Status-Type               Format Enum
    Name Acct-Delay-Time                Format Ulong
    Name Acct-Input-Octets              Format Ulong
    Name Acct-Output-Octets             Format Ulong
    Name Acct-Session-Id                Format String
    Name Acct-Authentic                 Format Enum
    Name Acct-Session-Time              Format Ulong
    Name Acct-Input-Packets             Format Ulong
    Name Acct-Output-Packets            Format Ulong
    Name Acct-Terminate-Cause           Format Enum
    Name Multilink-Session-ID           Format String
    Name Acct-Link-Count                Format Ulong
    Name Acct-Input-Giga-Words          Format Ulong
    Name Acct-Output-Giga-Words         Format Ulong
    Name Event-Timestamp                Format Ulong
    Name CHAP-Challenge                 Format Binary
    Name NAS-Port-Type                  Format Enum
    Name Port-Limit                     Format Ulong
    Name Tunnel-Type                    Format Enum
    Name Tunnel-Medium-Type             Format Enum
    Name Tunnel-Client-Endpoint         Format String
    Name Tunnel-Server-Endpoint         Format String
    Name Acct-Tunnel-Connection         Format String
    Name Tunnel-Password                Format Binary
    Name Prompt                         Format Enum
    Name Connect-Info                   Format String
    Name EAP-Message                    Format Binary
    Name Message-Authenticator          Format Binary
    Name Tunnel-Private-Group-Id        Format String
    Name Tunnel-Assignment-Id           Format String
    Name Tunnel-Preference              Format Ulong
    Name Acct-Interim-Interval          Format Ulong
    Name Tunnel-Packets-Lost            Format Ulong
    Name NAS-Port-Id                    Format String
    Name Tunnel-Client-Auth-ID          Format String
    Name Tunnel-Server-Auth-ID          Format String
    Name Framed-Interface-Id            Format Binary
    Name Framed-IPv6-Prefix             Format Binary
    Name login-ip-addr-host             Format Binary
    Name Framed-IPv6-Route              Format String
    Name Framed-IPv6-Pool               Format String
    Name Dynamic-Author-Error-Cause     Format Enum

Non Standard ATTRIBUTE LIST:
    Name Old-Password                   Format Binary
    Name Ascend-Filter-Required         Format Enum
    Name Ascend-Cache-Refresh           Format Enum
    Name Ascend-Cache-Time              Format Ulong
    Name Ascend-Auth-Type               Format Ulong
    Name Ascend-Redirect-Number         Format String
    Name Ascend-Private-Route           Format String
    Name Ascend-Shared-Profile-Enable   Format Boolean
    Name Ascend-Client-Primary-DNS      Format IPv4 Address
    Name Ascend-Client-Secondary-DNS    Format IPv4 Address
    Name Ascend-Client-Assign-DNS       Format Ulong
    Name Ascend-Session-Svr-Key         Format String
    Name Ascend-Multicast-Rate-Limit    Format Ulong
    Name Ascend-Multicast-Client        Format Ulong
    Name Ascend-Multilink-Session-ID    Format Ulong
    Name Ascend-Num-In-Multilink        Format Ulong
    Name Ascend-Presession-Octets-In    Format Ulong
    Name Ascend-Presession-Octets-Out   Format Ulong
```

```
    Name Ascend-Presession-Packets-In   Format Ulong
    Name Ascend-Presession-Packets-Out  Format Ulong
    Name Ascend-Max-Time                Format Ulong
    Name Ascend-Disconnect-Cause        Format Enum
    Name Ascend-Connection-Progress     Format Enum
    Name Ascend-Data-Rate               Format Ulong
    Name Ascend-Presession-Time         Format Ulong
    Name Ascend-Require-Auth            Format Ulong
    Name Ascend-PW-Liftime              Format Ulong
    Name Ascend-IP-Direct               Format IPv4 Address
    Name Ascend-PPP-VJ-Slot-Comp        Format Boolean
    Name Ascend-Asyncmap                Format Ulong
    Name Ascend-Send-Secret             Format Binary
    Name ascend_pool_definition         Format String
    Name Ascend-IP-Pool                 Format Ulong
    Name Ascend-Dial-Number             Format String
    Name Ascend-Route-IP                Format Boolean
    Name Ascend-Send-Auth               Format Enum
    Name Ascend-Link-Compression        Format Enum
    Name Ascend-Target-Util             Format Ulong
    Name Ascend-Max-Channels            Format Ulong
    Name Ascend-Data-Filter             Format Binary
    Name Ascend-Call-Filter             Format Binary
    Name Ascend-Idle-Limit              Format Ulong
    Name Ascend-Data-Service            Format Ulong
    Name Ascend-Force-56                Format Ulong
    Name Ascend-Xmit-Rate               Format Ulong

Cisco VSA ATTRIBUTE LIST:
    Name Cisco AVpair                   Format String
    Name cisco-nas-port                 Format String
    Name fax_account_id_origin          Format String
    Name fax_msg_id                     Format String
    Name fax_pages                      Format String
    Name fax_modem_time                 Format String
    Name fax_connect_speed              Format String
    Name fax_mdn_address                Format String
    Name fax_mdn_flag                   Format String
    Name fax_auth_status                Format String
    Name email_server_address           Format String
    Name email_server_ack_flag          Format String
    Name gateway_id                     Format String
    Name call_type                      Format String
    Name port_used                      Format String
    Name abort_cause                    Format String
    Name h323-remote-address            Format String
    Name Conf-Id                        Format String
    Name h323-setup-time                Format String
    Name h323-call-origin               Format String
    Name h323-call-type                 Format String
    Name h323-connect-time              Format String
    Name h323-disconnect-time           Format String
    Name h323-disconnect-cause          Format String
    Name h323-voice-quality             Format String
    Name h323-gw-id                     Format String
    Name Cisco AVpair                   Format Binary
    Name Cisco encrypted string vsa     Format String
    Name Sub_Policy_In                  Format String
    Name Sub_Policy_Out                 Format String
    Name h323-credit-amount             Format String
    Name h323-credit-time               Format String
    Name h323-return-code               Format String
    Name h323-prompt-id                 Format String
    Name h323-time-and-day              Format String
```

```
    Name h323-redirect-number           Format String
    Name h323-preferred-lang            Format String
    Name h323-redirect-ip-address       Format String
    Name h323-billing-model             Format String
    Name h323-currency                  Format String
    Name ssg-account-info               Format String
    Name ssg-service-info               Format String
    Name ssg-command-code               Format Binary
    Name ssg-control-info               Format String

Microsoft VSA ATTRIBUTE LIST:
    Name MS-CHAP-Response               Format Binary
    Name MS-CHAP-ERROR                  Format Binary
    Name MS-CHAP-CPW-1                  Format Binary
    Name MS-CHAP-CPW-2                  Format Binary
    Name MS-CHAP-LM-Enc-PW              Format Binary
    Name MS-CHAP-NT-Enc-PW              Format Binary
    Name MS-MPPE-Enc-Policy             Format Binary
    Name MS-MPPE-Enc-Type               Format Binary
    Name MS-RAS-Vendor                  Format String
    Name MS-CHAP-DOMAIN                 Format String
    Name MSCHAP_Challenge               Format Binary
    Name MS-CHAP-MPPE-Keys              Format Binary
    Name MS-BAP-Usage                   Format Binary
    Name MS-Link-Util-Thresh            Format Binary
    Name MS-Link-Drop-Time-Limit        Format Binary
    Name MS-MPPE-Send-Key               Format Binary
    Name MS-MPPE-Recv-Key               Format Binary
    Name MS-RAS-Version                 Format String
    Name MS-Old-ARAP-Password           Format Binary
    Name New-ARAP-Password              Format Binary
    Name MS-ARAP-PW-Change-Reason       Format Binary
    Name MS-Filter                      Format Binary
    Name MS-Acct-Auth-Type              Format Binary
    Name MS-MPPE-EAP-Type               Format Binary
    Name MS-CHAP-V2-Response            Format Binary
    Name MS-CHAP-V2-Success             Format String
    Name MS-CHAP-CPW-2                  Format Binary
    Name MS-Primary-DNS                 Format IPv4 Address
    Name MS-Secondary-DNS               Format IPv4 Address
    Name MS-1st-NBNS-Server             Format IPv4 Address
    Name MS-2nd-NBNS-Server             Format IPv4 Address
    Name MS-ARAP-Challenge              Format Binary

3GPP VSA ATTRIBUTE LIST:
    Name Charging-ID                    Format Ulong
    Name PDP Type                       Format Enum
    Name Charging-Gateway-Address       Format IPv4 Address
    Name GPRS-QoS-Profile               Format String
    Name SGSN-Address                   Format IPv4 Address
    Name GGSN-Address                   Format IPv4 Address
    Name IMSI-MCC-MNC                   Format String
    Name GGSN-MCC-MNC                   Format String
    Name NSAPI                          Format String
    Name Session-Stop-Ind               Format Binary
    Name Selection-Mode                 Format String
    Name Charging-Characteristics       Format String

3GPP2 VSA ATTRIBUTE LIST:
    Name cdma-reverse-tnl-spec          Format Ulong
    Name cdma-diff-svc-class-opt        Format Ulong
    Name cdma-container                 Format String
    Name cdma-ha-ip-addr                Format IPv4 Address
    Name cdma-pcf-ip-addr               Format IPv4 Address
```

```
    Name cdma-bs-msc-addr               Format String
    Name cdma-user-id                   Format Ulong
    Name cdma-forward-mux               Format Ulong
    Name cdma-reverse-mux               Format Ulong
    Name cdma-forward-rate              Format Ulong
    Name cdma-reverse-rate              Format Ulong
    Name cdma-service-option            Format Ulong
    Name cdma-forward-type              Format Ulong
    Name cdma-reverse-type              Format Ulong
    Name cdma-frame-size                Format Ulong
    Name cdma-forward-rc                Format Ulong
    Name cdma-reverse-rc                Format Ulong
    Name cdma-ip-tech                   Format Ulong
    Name cdma-comp-flag                 Format Enum
    Name cdma-reason-ind                Format Enum
    Name cdma-bad-frame-count           Format Ulong
    Name cdma-num-active                Format Ulong
    Name cdma-sdb-input-octets          Format Ulong
    Name cdma-sdb-output-octets         Format Ulong
    Name cdma-numsdb-input              Format Ulong
    Name cdma-numsdb-output             Format Ulong
    Name cdma-ip-qos                    Format Ulong
    Name cdma-airlink-qos               Format Ulong
    Name cdma-rp-session-id             Format Ulong
    Name cdma-hdlc-layer-bytes-in       Format Ulong
    Name cdma-correlation-id            Format String
    Name cdma-moip-inbound              Format Ulong
    Name cdma-moip-outbound             Format Ulong
    Name cdma-session-continue          Format Ulong
    Name cdma-active-time               Format Ulong
    Name cdma-frame-size                Format Ulong
    Name cdma-esn                       Format String
    Name cdma-mn-ha-spi                 Format Ulong
    Name cdma-mn-ha-shared-key          Format Binary
    Name cdma-sess-term-capability      Format Ulong
    Name cdma-disconnect-reason         Format Ulong

Verizon VSA ATTRIBUTE LIST:
    Name mip-key-data                   Format Binary
    Name aaa-authenticator              Format Binary
    Name public-key-invalid             Format Binary
```

Table 179 describes the significant fields shown in the display.

Table 181 show radius table attributes Field Descriptions

Field	Description
User-Name	The name of the user on the system. The format is String.
User-Password	The password of the user on the system. The format is Binary.
CHAP-Password	Challenge Handshake Authentication Protocol (CHAP) password. The format is Binary.
NAS-IP-Address	Network-Attached Storage (NAS) IP address. The format is IPv4 Address.
NAS-Port	The RADIUS Attribute 5 (NAS-Port) format specified on a per-server group level. The format is Ulong.
Service-Type	Sets the service type. The format is Enum.

Table 181 show radius table attributes Field Descriptions (continued)

Field	Description
Framed-Protocol	Indicates the framing to be used for framed access. It may be used in both Access-Request and Access-Accept packets. The format is Enum.
Framed-IP-Address	Indicates the address to be configured for the user. It may be used in Access-Accept packets. The format is IPv4 Address.
Framed-IP-Netmask	Indicates the IP netmask to be configured for the user when the user is a router to a network. The format is IPv4 Address.
Framed-Routing	Indicates the routing method for the user when the user is a router to a network. The format is Ulong.
Filter-Id	To disable, enable, get, or set a filter, the filter ID must be valid. The format is Binary.
Framed-MTU	Indicates the maximum transmission unit to be configured for the user, when it is not negotiated by some other means (such as PPP). The format is Ulong.
Framed-Compression	Indicates a compression protocol to be used for the link. The format is Enum.
login-ip-addr-host	Indicates the host to which the user will connect when the Login-Service attribute is included. The format is IPv4 Address.
Login-Service	The Login-IP-Host AVP (AVP Code 14) is of type Address and contains the system with which to connect the user, when the Login-Service AVP is included. The format is Enum.
login-tcp-port	The Login-TCP-Port AVP (AVP Code 16) is of type Integer32 and contains the TCP port with which the user is to be connected, when the Login-Service AVP is also present. The format is Ulong.
Reply-Message	Indicates text that may be displayed to the user. The format is Binary.
Callback-Number	Indicates a dialing string to be used for callback. The format is String.
Framed-Route	Provides routing information to be configured for the user on the NAS. The format is String.
Framed-IPX-Network	The Framed-IPX-Network AVP (AVP Code 23) is of type Unsigned32, and contains the IPX Network number to be configured for the user. The format is Pv4 Address.
State	Is available to be sent by the server to the client in an Access-Challenge and must be sent unmodified from the client to the server in the new Access-Request reply to that challenge, if any. The format is Binary.
Class	Is available to be sent by the server to the client in an Access-Accept and should be sent unmodified by the client to the accounting server as part of the Accounting-Request packet if accounting is supported. The format is Binary.

Table 181 show radius table attributes Field Descriptions (continued)

Field	Description
Vendor-Specific	Is available to allow vendors to support their own extended attributes not suitable for general usage. The format is Binary.
Session-Timeout	Sets the maximum number of seconds of service to be provided to the user before termination of the session or prompt. The format is Ulong.
Idle-Timeout	Sets the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session or prompt. The format is Ulong.
Termination-Action	Indicates what action the NAS should take when the specified service is completed. The format is Boolean.
Called-Station-Id	The Called-Station-Id AVP (AVP Code 30) is of type String and allows the NAS to send in the request the phone number that the user called, using Dialed Number Identification (DNIS) or a similar technology. The format is String.
Calling-Station-Id	The Calling-Station-Id AVP (AVP Code 31) is of type String and allows the NAS to send in the request the phone number that the call came from, using Automatic Number Identification (ANI) or a similar technology. The format is String.
Nas-Identifier	Contains a string identifying the NAS originating the access request. The format is String.
Acct-Status-Type	Indicates whether this Accounting-Request marks the beginning of the user service (Start) or the end (Stop). The format is Enum.
Acct-Delay-Time	Indicates how many seconds the client has been trying to send this record for, and can be subtracted from the time of arrival on the server to find the approximate time of the event generating this Accounting-Request. (Network transit time is ignored.) The format is Ulong.
Acct-Input-Octets	Indicates how many octets have been received from the port over the course of this service being provided, and can only be present in Accounting-Request records where Acct-Status-Type is set to Stop. The format is Ulong.
Acct-Output-Octets	Indicates how many octets have been sent to the port in the course of delivering this service, and can only be present in Accounting-Request records where Acct-Status-Type is set to Stop. The format is Ulong.
Acct-Session-Id	Is a unique accounting ID to make it easy to match start and stop records in a log file. The format is String.
Acct-Authentic	Indicate how the user was authenticated, whether by Radius, the NAS itself, or another remote authentication protocol. It may be included in an Accounting-Request. The format is Enum.

Table 181 show radius table attributes Field Descriptions (continued)

Field	Description
Acct-Session-Time	Indicates how many seconds the user has received service for, and can only be present in Accounting-Request records where Acct-Status-Type is set to Stop. The format is Ulong.
Acct-Input-Packets	Indicates how many packets have been received from the port over the course of this service being provided to a framed user, and can only be present in Accounting-Request records where Acct-Status-Type is set to Stop. The format is Ulong.
Acct-Output-Packets	Indicates how many packets have been sent to the port in the course of delivering this service to a framed user, and can only be present in Accounting-Request records where Acct-Status-Type is set to Stop. The format is Ulong.
Acct-Terminate-Cause	Indicates how the session was terminated, and can only be present in Accounting-Request records where Acct-Status-Type is set to Stop. The format is Enum.
Multilink-Session-ID	Indicates the service to use to connect the user to the login host. It is only used in Access-Accept packets. The format is String.
Acct-Link-Count	Gives the count of links which are known to have been in a given multilink session at the time the accounting record is generated. The format is Ulong.
Acct-Input-Giga-Words	Indicates how many times the Acct-Input-Octets counter has wrapped around 2^32 over the course of this service being provided, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop or Interim-Update. The format is Ulong.
Acct-Output-Giga-Words	Indicates how many times the Acct-Output-Octets counter has wrapped around 2^32 in the course of delivering this service, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop or Interim-Update. The format is Ulong.
Event-Timestamp	Use to include the Event-Timestamp attribute in Acct-Start or Acct-Stop messages. The format is Ulong.
CHAP-Challenge	The CHAP is used to verify periodically the identity of the peer using a 3-way handshake. The format is Binary.
NAS-Port-Type	Indicates the physical port number of the NAS which is authenticating the user. The format is Enum.
Port-Limit	Sets the maximum number of ports to be provided to the user by the NAS. The format is Ulong.
Tunnel-Type	Indicates the tunneling protocol(s) to be used (in the case of a tunnel initiator) or the the tunneling protocol in use (in the case of a tunnel terminator). The format is Enum.
Tunnel-Medium-Type	Indicates which transport medium to use when creating a tunnel for those protocols (such as L2TP) that can operate over multiple transports. The format is Enum.

Table 181 show radius table attributes Field Descriptions (continued)

Field	Description
Tunnel-Client-Endpoint	Contains the address of the initiator end of the tunnel. The format is String.
Tunnel-Server-Endpoint	Indicates the address of the server end of the tunnel. The format is String.
Acct-Tunnel-Connection	Indicates the identifier assigned to the tunnel session. The format is String.
Tunnel-Password	Can contain a password to be used to authenticate to a remote server. The format is Binary.
Prompt	Used only in Access-Challenge packets, and indicates to the NAS whether it should echo the user's response as it is entered, or not echo it. The format is Enum.
Connect-Info	Is sent from the NAS to indicate the nature of the user's connection. The format is String.
EAP-Message	Encapsulates Extensible Authentication Protocol packets so as to allow the NAS to authenticate dial-in users via EAP without having to understand the protocol. The format is Binary.
Message-Authenticator	Can be used to authenticate and integrity-protect Access-Requests in order to prevent spoofing. The format is Binary.
Tunnel-Private-Group-Id	Indicates the group ID for a particular tunneled session. The format is String.
Tunnel-Assignment-Id	Used to indicate to the tunnel initiator the particular tunnel to which a session is to be assigned. The format is String.
Tunnel-Preference	Should be included in each set to indicate the relative preference assigned to each tunnel if more than one set of tunneling attributes is returned by the RADIUS server to the tunnel initiator. The format is Ulong.
Acct-Interim-Interval	Indicates the number of seconds between each interim update in seconds for this specific session. The format is Ulong.
Tunnel-Packets-Lost	Indicates the number of packets lost on a given link. The format is Ulong.
NAS-Port-Id	Used to identify the IEEE 802.1X Authenticator port which authenticates the Supplicant. The format is String.
Tunnel-Client-Auth-ID	Specifies the name used by the tunnel initiator during the authentication phase of tunnel establishment. The format is String.
Tunnel-Server-Auth-ID	Specifies the name used by the tunnel terminator during the authentication phase of tunnel establishment. The format is String.
Framed-Interface-Id	Indicates the IPv6 interface identifier to be configured for the user. The format is Binary.

Table 181 show radius table attributes Field Descriptions (continued)

Field	Description
Framed-IPv6-Prefix	Indicates an IPv6 prefix (and corresponding route) to be configured for the user. The format is Binary.
Framed-IPv6-Route	Provides routing information to be configured for the user on the NAS. The format is String.
Framed-IPv6-Pool	Contains the name of an assigned pool that should be used to assign an IPv6 prefix for the user. The format is String.
Dynamic-Author-Error-Cause	Specifies the error causes associated with dynamic authorization. The format is Enum.
Old-Password	Is 16 octets in length. It contains the encrypted Lan Manager hash of the old password. The format is Binary.
Ascend-Filter-Required	Specifies whether the call should be permitted if the specified filter is not found. If present, this attribute will be applied after any authentication, authorization, and accounting (AAA) filter method-list. The format is Enum.
Ascend-Cache-Refresh	Specifies whether cache entries should be refreshed each time an entry is referenced by a new session. This attribute corresponds to the **cache refresh** command. The format is Enum.
Ascend-Cache-Time	Specifies the idle time out, in minutes, for cache entries. This attribute corresponds to the **cache clear age** command. The format is Ulong.
Ascend-Auth-Type	Indicates the type of name and password (PPP) authorization to use. The format Ulong.
Ascend-Redirect-Number	Indicates the original number in the information sent to the authentication server when the number dialed by a device is redirected to another number for authentication. The format is String.
Ascend-Private-Route	Specifies whether IP routing is allowed for the user profile. The format is String.
Ascend-Shared-Profile-Enable	Specifies whether multiple incoming callers can share a single RADIUS user profile. The format is Boolean.
Ascend-Client-Primary-DNS	Specifies a primary DNS server address to send to any client connecting to the MAX TNT. The format is IPv4 Address.
Ascend-Client-Secondary-DNS	Specifies a secondary DNS server address to send to any client connecting to the MAX TNT. The format is IPv4 Address.
Ascend-Client-Assign-DNS	Specifies whether or not the MAX TNT sends the Ascend-Client-Primary-DNS and Ascend-Client-Secondary-DNS values during connection negotiation. The format is Ulong.
Ascend-Session-Svr-Key	Specifies the session key that identifies the user session. You can specify up to 16 characters. The default value is null. The format is String.

Table 181 show radius table attributes Field Descriptions (continued)

Field	Description
Ascend-Multicast-Rate-Limit	Specifies how many seconds the MAX waits before accepting another packet from the multicast client. The format is Ulong.
Ascend-Multicast-Client	Specifies whether the user is a multicast client of the MAX. The format is Ulong.
Ascend-Multilink-Session-ID	Specifies the ID number of the Multilink bundle when the session closes. A Multilink bundle is a multichannel MP or MP+ call. The format is Ulong.
Ascend-Num-In-Multilink	Indicates the number of sessions remaining in a Multilink bundle when the session closes. A Multilink bundle is a multichannel MP or MP+ call. The format is Ulong.
Ascend-Presession-Octets-In	Reports the number of octets received before authentication. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet. The format is Ulong.
Ascend-Presession-Octets-Out	Reports the number of octets transmitted before authentication. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet. The format is Ulong.
Ascend-Presession-Packets-In	Reports the number of packets received before authentication. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets. The format is Ulong.
Ascend-Presession-Packets-Out	Reports the number of packets transmitted before authentication. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets. The format is Ulong.
Ascend-Max-Time	Specifies the maximum length of time in seconds that any session can remain online. Once a session reaches the time limit, its connection goes offline. The format is Ulong.
Ascend-Disconnect-Cause	Indicates the reason a connection went offline. The format is Enum.
Ascend-Connection-Progress	Indicates the state of the connection before it disconnects. The format is Enum.
Ascend-Data-Rate	Specifies the rate of data received on the connection in bits per second. The format is Ulong.
Ascend-Presession-Time	Reports the length of time in seconds from when a call connected to when it completes authentication. The format is Ulong.

Table 181 show radius table attributes Field Descriptions (continued)

Field	Description
Ascend-Require-Auth	Specifies whether the MAX TNT requires additional authentication after Calling-Line ID (CLID) or called-number authentication. The format is Ulong.
Ascend-PW-Liftime	Specifies the number of days that a password is valid. The format is Ulong.
Ascend-IP-Direct	Specifies the IP address to which the MAX TNT redirects packets from the user. When you include this attribute in a user profile, the MAX TNT bypasses all internal routing tables, and simply sends all packets it receives on the connection's WAN interface to the specified IP address. The format is IPv4 Address.
Ascend-PPP-VJ-Slot-Comp	Instructs the MAX TNT to not use slot compression when sending VJ-compressed packets. The format is Boolean.
Ascend-Asyncmap	The format is Ulong.
Ascend-Send-Secret	Specifies the password that the RADIUS server sends to the remote end of a connection on an outgoing call. It is encrypted when passed between the RADIUS server and the MAX TNT. The format is Binary.
Ascend_pool_definition	Specifies all the addresses in the pool. The format is String.
Ascend-IP-Pool	Specifies the first address in an IP address pool, as well as the number of addresses in the pool. The format is Ulong.
Ascend-Dial-Number	Specifies the phone number the MAX TNT dials to reach the router or node at the remote end of the link. The format is String.
Ascend-Route-IP	Specifies whether IP routing is allowed for the user profile. The format is Boolean.
Ascend-Send-Auth	Specifies the authentication protocol that the MAX TNT requests when initiating a PPP or MP+ connection. The answering side of the connection determines which authentication protocol, if any, the connection uses. The format is Enum.
Ascend-Link-Compression	Turns data compression on or off for a PPP link. The format is Enum.
Ascend-Target-Util	Specifies the percentage of bandwidth use at which the MAX TNT adds or subtracts bandwidth. The format is Ulong.
Ascend-Max-Channels	Specifies the maximum number of channels allowed on an MP+ call. The format is Ulong.
Ascend-Data-Filter	Specifies the characteristics of a data filter in a RADIUS user profile. The MAX TNT uses the filter only when it places or receives a call associated with the profile that includes the filter definition. The format is Binary.

Table 181 show radius table attributes Field Descriptions (continued)

Field	Description
Ascend-Call-Filter	Specifies the characteristics of a call filter in a RADIUS user profile. The MAX TNT uses the filter only when it places a call or receives a call associated with the profile that includes the filter definition. The format is Binary.
Ascend-Idle-Limit	Specifies the number of seconds the MAX TNT waits before clearing a call when a session is inactive. The format is Ulong.
Ascend-Data-Service	Specifies the type of data service the link uses for outgoing calls. The format is Ulong.
Ascend-Force-56	Indicates whether the MAX uses only the 56-kbps portion of a channel, even when all 64-kbps appear to be available. The format is Ulong.
Ascend-Xmit-Rate	Specifies the rate of data transmitted on the connection in bits per second. For ISDN calls, Ascend-Xmit-Rate indicates the transmit data rate. For analog calls, it indicates the modem baud rate at the time of the initial connection. The format is Ulong.
Cisco AVpair	The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. Cisco's vendor-ID is 9, and the supported option has vendor-type 1, which is named “cisco-avpair”. The format is String.
cisco-nas-port	Enables the display of physical interface information and parent interface details as part of the of the cisco-nas-port vendor-specific attribute (VSA) for login calls. The format is String.
fax_account_id_origin	Indicates the account ID origin as defined by system administrator for the **mmoip aaa receive-id** or the **mmoip aaa send-id** command. The format is String.
fax_msg_id	Indicates a unique fax message identification number assigned by Store and Forward Fax. The format is String.
fax_pages	Indicates the number of pages transmitted or received during this fax session. This page count includes cover pages. The format is String.
fax_modem_time	Indicates the amount of time in seconds the modem sent fax data (x) and the amount of time in seconds of the total fax session (y), which includes both fax-mail and PSTN time, in the form x/y. For example, 10/15 means that the transfer time took 10 seconds, and the total fax session took 15 seconds. The format is String.
fax_connect_speed	Indicates the modem speed at which this fax-mail was initially transmitted or received. Possible values are 1200, 4800, 9600, and 14400. The format is String.
fax_mdn_address	Indicates the address to which message delivery notifications (MDNs) will be sent. The format is String.

Table 181 show radius table attributes Field Descriptions (continued)

Field	Description
fax_mdn_flag	Indicates whether or not MDNs has been enabled. True indicates that MDN had been enabled; false means that MDN had not been enabled. The format is String.
fax_auth_status	Indicates whether or not authentication for this fax session was successful. Possible values for this field are success, failed, bypassed, or unknown. The format is String.
email_server_address	Indicates the IP address of the e-mail server handling the on-ramp fax-mail message. The format is String.
email_server_ack_flag	Indicates that the on-ramp gateway has received a positive acknowledgment from the e-mail server accepting the fax-mail message. The format is String.
gateway_id	Indicates the name of the gateway that processed the fax session. The name appears in the following format: hostname.domain-name. The format is String.
call_type	Describes the type of fax activity: fax receive or fax send. The format is String.
port_used	Indicates the slot/port number of the Cisco AS5300 used to either transmit or receive this fax-mail. The format is String.
abort_cause	If the fax session aborts, indicates the system component that signaled the abort. Examples of system components that could trigger an abort are FAP (Fax Application Process), TIFF (the TIFF reader or the TIFF writer), fax-mail client, fax-mail server, ESMTP client, or ESMTP server. The format is String.
h323-remote-address	Indicates the IP address of the remote gateway. The format is String.
Conf-Id	Indicates a unique call identifier generated by the gateway. Used to identify the separate billable events (calls) within a single calling session. The format is String.
h323-setup-time	Indicates the setup time in NTP format: hour, minutes, seconds, microseconds, time_zone, day, month, day_of_month, year. The format is String.
h323-call-origin	Indicates the gateway's behavior in relation to the connection that is active for this leg. The format is String.
h323-call-type	Indicates the protocol type or family used on this leg of the call. The format is String.
h323-connect-time	Indicates the connect time in Network Time Protocol (NTP) format: hour, minutes, seconds, microseconds, time_zone, day, month, day_of_month, and year. The format is String.
h323-disconnect-time	Indicates the disconnect time in NTP format: hour, minutes, seconds, microseconds, time_zone, day, month, day_of_month, year. The format is String.

Table 181 show radius table attributes Field Descriptions (continued)

Field	Description
h323-disconnect-cause	Indicates the Q.931 disconnect cause code retrieved from CCAPI. The source of the code is the disconnect location such as a PSTN, terminating gateway, or SIP. The format is String.
h323-voice-quality	Indicates the ICPIF of the voice quality. The format is String.
h323-gw-id	Indicate the name of the tenor. The format is String.
Cisco AVpair	The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. Cisco's vendor-ID is 9, and the supported option has vendor-type 1, which is named “cisco-avpair”. The format is String.
Cisco encrypted string vsa	Cisco allows several forms of sub-attribute encryption. The only method supported is the Cisco Encrypted String VSA Format also supported by an IETF draft for Salt-Encryption of RADIUS attributes. The format is String.
Sub_Policy_In	Defines the service policy input. The format is String.
Sub_Policy_Out	Defines the service policy output. The format is String.
h323-credit-amount	Indicates the amount of credit (in currency) that the account contains. The format is String.
h323-credit-time	Indicates the number of seconds for which the call is authorized. The format is String.
h323-return-code	Return codes are instructions from the RADIUS server to the voice gateway. The format is String.
h323-prompt-id	Indexes into an array that selects prompt files used at the gateway. The format is String.
h323-time-and-day	Indicates the time of day at the dialed number or at the remote gateway in the format: hour, minutes, seconds. The format is String.
h323-redirect-number	Indicates the phone number to which the call is redirected; for example, to a toll-free number or a customer service number. The format is String.
h323-preferred-lang	Indicates the language to use when playing the audio prompt specified by the h323-prompt-id. The format is String.
h323-redirect-ip-address	Indicates the IP address for an alternate or redirected call. The format is String.
h323-billing-model	Indicates the type of billing service for a specific call. The format is String.
h323-currency	Indicates the currency to use with h323-credit-amount. The format is String.
ssg-account-info	Subscribes the subscriber to the specified service and indicates that the subscriber should be automatically connected to this service after successful logon. The format is String.

Table 181 show radius table attributes Field Descriptions (continued)

Field	Description
ssg-service-info	SSG redirects the user's HTTP traffic to a server in the specified server group. All the service features (such as quality of service (QoS) and prepaid billing) are applied to the HTTP traffic. The format is String.
ssg-command-code	Specifies account logon and logoff, session query, and service activate and deactivate information. The format is Binary.
ssg-control-info	Indicates the control-info code for prepaid quota. The format is String.
MS-CHAP-Response	This attribute contains the response value provided by a PPP Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP) user in response to the challenge. The format is Binary.
MS-CHAP-ERROR	Contains error data related to the preceding MS-CHAP exchange. The format is Binary.
MS-CHAP-CPW-1	Allows the user to change their password if it has expired. The format is Binary.
MS-CHAP-CPW-2	Allows the user to change their password if it has expired. The format is Binary.
MS-CHAP-LM-Enc-PW	Contains the new Windows NT password encrypted with the old LAN Manager password hash. The format is Binary.
MS-CHAP-NT-Enc-PW	Contains the new Windows NT password encrypted with the old Windows NT password hash. The format is Binary.
MS-MPPE-Enc-Policy	The MS-MPPE-Encryption-Policy attribute may be used to signify whether the use of encryption is allowed or required. The format is Binary.
MS-MPPE-Enc-Type	The MS-MPPE-Encryption-Types attribute is used to signify the types of encryption available for use with Microsoft Point-to-Point Encryption (MPPE). The format is Binary.
MS-RAS-Vendor	Used to indicate the manufacturer of the RADIUS client machine. The format is Binary.
MS-CHAP-DOMAIN	Indicates the Windows NT domain in which the user was authenticated. The format is Binary.
MSCHAP_Challenge	Contains the challenge sent by a NAS to a MS-CHAP user. The format is Binary.
MS-CHAP-MPPE-Keys	Contains two session keys for use by the MPPE. The format is Binary.
MS-BAP-Usage	Describes whether the use of Bandwidth Allocation Protocol (BAP) is allowed, disallowed or required on new multilink calls. The format is Binary.
MS-Link-Util-Thresh	Represents the percentage of available bandwidth utilization below which the link must fall before the link is eligible for termination. The format is Binary.

Table 181 show radius table attributes Field Descriptions (continued)

Field	Description
MS-Link-Drop-Time-Limit	Indicates the length of time (in seconds) that a link must be underutilized before it is dropped. The format is Binary.
MS-MPPE-Send-Key	Contains a session key for use by the MPPE. The format is Binary.
MS-MPPE-Recv-Key	Contains a session key for use by the MPPE. The format is Binary.
MS-RAS-Version	Used to indicate the version of the RADIUS client software. The format is Binary.
MS-Old-ARAP-Password	Used to transmit the old Apple Remote Access Protocol (ARAP) password during an ARAP password change operation. The format is Binary.
New-ARAP-Password	Used to transmit the new ARAP password during an ARAP password change operation. The format is Binary.
MS-ARAP-PW-Change-Reason	Used to indicate reason for a server-initiated password change. The format is Binary.
MS-Filter	Used to transmit traffic filters. The format is Binary.
MS-Acct-Auth-Type	Used to represent the method used to authenticate the dial-up user. The format is Binary.
MS-MPPE-EAP-Type	Used to represent the EAP type used to authenticate the dial-up user. The format is Binary.
MS-CHAP-V2-Response	This attribute is identical in format to the standard CHAP Response packet. The format is Binary.
MS-CHAP-V2-Success	Contains a 42-octet authenticator response string and must be included in the Message field packet sent from the NAS to the peer. The format is Binary.
MS-CHAP-CPW-2	Allows the user to change their password if it has expired. The format is Binary.
MS-Primary-DNS	Used to indicate the address of the primary DNS server to be used by the PPP peer. The format is IPv4 Address.
MS-Secondary-DNS	Used to indicate the address of the secondary DNS server to be used by the PPP peer. The format is IPv4 Address.
MS-1st-NBNS-Server	Used to indicate the address of the primary NetBIOS Name Server (NBNS) server to be used by the PPP peer. The format is IPv4 Address.
MS-2nd-NBNS-Server	Used to indicate the address of the secondary NBNS server to be used by the PPP peer. The format is IPv4 Address.
MS-ARAP-Challenge	Only present in an Access-Request packet containing a Framed-Protocol Attribute with the value 3 (ARAP). The format is Binary.
Charging-ID	Generated for each activated context. It is a unique four octet value generated by the GGSN when a PDP Context is activated. The format is Ulong.

Table 181 show radius table attributes Field Descriptions (continued)

Field	Description
PDP Type	Indicates the Packet Data Protocol (PDP) is to be used by the mobile for a certain service. The format is Enum.
Charging-Gateway-Address	The IP address of the recommended Charging Gateway Functionality to which the SGSN should transfer the Charging Detail Records (CDR) for this PDP Context. The format is IPv4 Address.
GPRS-QoS-Profile	Controls the QoS negotiated values. The format is String.
SGSN-Address	This is the IP address of the SGSN that is used by the GTP control plane for handling control messages. The format is IPv4 Address.
GGSN-Address	IP address of the GGSN that is used by the GTP control plane for the context establishment. This address is the same as the GGSN IP address used in G-CDRs. The format is IPv4 Address.
IMSI-MCC-MNC	The MCC and MNC extracted from the user's IMSI number (the first 5 or 6 digits depending on the IMSI). The format is String.
GGSN-MCC-MNC	The MCC and MNC of the network to which the GGSN belongs. The format is String.
NSAPI	Identifies a particular PDP context for the associated PDN and MSISDN/IMSI from creation to deletion. The format is String.
Session-Stop-Ind	Indicates to the AAA server that the last PDP context of a session is released and that the PDP session has been terminated. The format is Binary
Selection-Mode	Contains the selection mode for this PDP Context received in the Create PDP Context Request Message. The format is String.
Charging-Characteristics	Contains the charging characteristics for this PDP Context received in the Create PDP Context Request Message (only available in R99 and later releases). The format is String.
cdma-reverse-tnl-spec	Indicates the style of reverse tunneling that is required, and optionally appears in a RADIUS Access-Accept message. The format is Ulong.
cdma-diff-svc-class-opt	This attribute is deprecated and is replaced by the Allowed Differentiated Services Marking attribute. The Home RADIUS server authorizes differentiated services via the Differentiated Services Class Options attribute, and optionally appears in a RADIUS Access-Accept message. The format is Ulong.
cdma-container	Contains embedded 3GPP2 VSAs and/or RADIUS accounting attributes. The format is String.

Table 181 show radius table attributes Field Descriptions (continued)

Field	Description
cdma-ha-ip-addr	A Home Agent (HA) IP address used during a MIP session by the user as defined in IETF RFC 2002. The format is IPv4 Address.
cdma-pcf-ip-addr	The IP address of the serving PCF (the PCF in the serving RN). The format is IPv4 Address.
cdma-bs-msc-addr	The Base Station (BS) Mobile Switching Center (MSC) address. The format is String.
cdma-user-id	The name of the user on the system. The format is Ulong.
cdma-forward-mux	Forwards FCH multiplex option. The format is Ulong.
cdma-reverse-mux	Reverses FCH multiplex option. The format is Ulong.
cdma-forward-rate	The format and structure of the radio channel in the forward Dedicated Control Channel. A set of forward transmission formats that are characterized by data rates, modulation characterized, and spreading rates. The format is Ulong.
cdma-reverse-rate	The format and structure of the radio channel in the reverse Dedicated Control Channel. A set of reverse transmission formats that are characterized by data rates, modulation characterized, and spreading rates. The format is Ulong.
cdma-service-option	Code Division Multiple Access (CDMA) service option as received from the RN. The format is Ulong.
cdma-forward-type	Forward direction traffic type. It is either Primary or Secondary. The format is Ulong.
cdma-reverse-type	Reverse direction traffic type. It is either Primary or Secondary. The format is Ulong.
cdma-frame-size	Specifies the Fundamental Channel (FCH) frame size. The format is Ulong.
cdma-forward-rc	The format and structure of the radio channel in the forward FCH. A set of forward transmission formats that are characterized by data rates, modulation characterized, and spreading rates. The format is Ulong.
cdma-reverse-rc	The format and structure of the radio channel in the reverse FCH. A set of reverse transmission formats that are characterized by data rates, modulation characterized, and spreading rates. The format is Ulong.
cdma-ip-tech	Identifies the IP technology to use for the call: Simple IP or Mobile IP. The format is Ulong.
cdma-comp-flag	Indicates the type of compulsory tunnel. The format is Ulong.
cdma-reason-ind	Indicates the reasons for a stop record. The format is Ulong.
cdma-bad-frame-count	The total number of PPP frames from the MS dropped by the Packet Data Serving Node (PDSN) due to uncorrectable errors. The format is Ulong.
cdma-num-active	The number of active transitions. The format is Ulong.

Table 181 show radius table attributes Field Descriptions (continued)

Field	Description
cdma-sdb-input-octets	This is the Short Data Burst (SDB) octet count reported by the RN in the SDB Airlink Record. The format is Ulong.
cdma-sdb-output-octets	The SDB octet count reported by the RN in the SDB Airlink Record. The format is Ulong.
cdma-numsdb-input	The number of terminating SDBs. The format is Ulong.
cdma-numsdb-output	The number of originating SDBs. The format is Ulong.
cdma-ip-qos	Indicates the IP Quality of Service (QoS). The format is Ulong.
cdma-airlink-qos	Identifies Airlink Priority associated with the user. This is the user's priority associated with the packet data service. The format is Ulong.
cdma-rp-session-id	Identifies the resource reservation protocol type session identifier. The format is Ulong.
cdma-hdlc-layer-bytes-in	The count of all octets received in the reverse direction by the High-Level Data Link Control (HDLC) layer in the PDSN. The format is Ulong.
cdma-correlation-id	Indicates a unique accounting ID created by the Serving PDSN for each packet data session that allows multiple accounting events for each associated R-P connection or P-P connection to be correlated.The format is String.
cdma-moip-inbound	This is the total number of octets in registration requests and solicitations sent by the MS. The format is Ulong.
cdma-moip-outbound	This is the total number of octets in registration replies and agent advertisements, sent to the MS. The format is Ulong.
cdma-session-continue	This attribute when set to “true” means it is not the end of a Session and an Accounting Stop is immediately followed by an Account Start Record. “False” means end of a session. The format is Ulong.
cdma-active-time	The total active connection time on traffic channel in seconds. The format is Ulong.
cdma-frame-size	Specifies the FSH frame size. The format is Ulong.
cdma-esn	Indicates the Electronic Serial Number (ESN). The format is String.
cdma-mn-ha-spi	The SPI for the MN-HA shared key that optionally appears in a RADIUS Access-Request message. It is used to request an MN-HA shared key. The format is Ulong.
cdma-mn-ha-shared-key	A shared key for MN-HA that may appear in a RADIUS Access-Accept message. The MN-HA shared key is encrypted using a method based on the RSA Message Digest Algorithm MD5 [RFC 1321] as described in Section 3.5 of RFC 2868. The format is Binary.

Table 181 show radius table attributes Field Descriptions (continued)

Field	Description
cdma-sess-term-capability	The value shall be bitmap encoded rather than a raw integer. This attribute shall be included in a RADIUS Access-Request message to the Home RADIUS server and shall contain the value 3 to indicate that the PDSN and HA support both Dynamic authorization with RADIUS and Registration Revocation for Mobile IPv4. The attribute shall also be included in the RADIUS Access-Accept message and shall contain the preferred resource management mechanism by the home network, which shall be used for the session and may include values 1 to 3. The format is Ulong.
cdma-disconnect-reason	Indicates the reason for disconnecting the user. This attribute may be included in a RADIUS Disconnect-Request message from Home RADIUS server to the PDSN. The format is Ulong.
mip-key-data	This is the key data payload containing the encrypted MN_AAA key, MN_HA key, CHAP key, MN_Authenticator, and AAA_Authenticator. The format is Binary.
aaa-authenticator	This is the 64-bit AAA_Authenticator value decrypted by the Home RADIUS AAA Server. The format is Binary.
public-key-invalid	The home RADIUS AAA Server includes this attribute to indicate that the Public key used by the MN is not valid. The format is Binary.

Related Commands

Command	Description
show radius	Displays information about the RADIUS servers that are configured in the system.

show redundancy application control-interface group

To display control interface information for a redundancy group, use the **show redundancy application control-interface group** command in privileged EXEC mode.

show redundancy application control-interface group [*group-id*]

Syntax Description

group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application control-interface** command shows information for the redundancy group control interfaces.

Examples

The following is sample output from the **show redundancy application control-interface** command:

```
Router# show redundancy application control-interface group 2

The control interface for rg[2] is GigabitEthernet0/1/0
Interface is Control interface associated with the following protocols: 2 1
BFD Enabled
Interface Neighbors:
```

Related Commands

Command	Description
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application group	Displays redundancy group information.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.
show redundancy application protocol	Displays protocol-specific information for a redundancy group.

show redundancy application data-interface

To display data interface-specific information, use the **show redundancy application data-interface** command in privileged EXEC mode.

show redundancy application data-interface group [*group-id*]

Syntax Description

group	Specifies the redundancy group.
group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application data-interface** command displays information about the redundancy group data interfaces.

Examples

The following is sample output from the **show redundancy application data-interface** command:

```
Router# show redundancy application data-interface group 1

The data interface for rg[1] is GigabitEthernet0/1/1
```

Related Commands

Command	Description
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application group	Displays redundancy group information.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.
show redundancy application protocol	Displays protocol-specific information for a redundancy group.

show redundancy application faults group

To display fault-specific information for a redundancy group, use the **show redundancy application faults group** command in privileged EXEC mode.

show redundancy application faults group [*group-id*]

Syntax Description

group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application faults** command shows information returned by redundancy group faults.

Examples

The following is sample output from the **show redundancy application faults** command:

```
Router# show redundancy application faults group 2

Faults states Group 2 info:
        Runtime priority: [150]
                RG Faults RG State: Up.
                        Total # of switchovers due to faults:           2
                        Total # of down/up state changes due to faults: 2
```

Table 182 describes the significant fields shown in the display.

Table 182 show redundancy application group all Field Descriptions

Field	Description
Faults states Group 1 info	Redundancy group faults information for Group 1.
Runtime priority	Current redundancy group priority of the group. This field is important when monitoring redundancy group switchover and when configuring interface tracking.
RG Faults RG State	Redundancy group state returned by redundancy group faults.
Total # of switchovers due to faults	Number of switchovers triggered by redundancy group fault events.
Total # of down/up state changes due to faults	Number of down and up state changes triggered by redundancy group fault events.

Related Commands

Command	Description
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application group	Displays redundancy group information.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.
show redundancy application protocol	Displays protocol-specific information for a redundancy group.

show redundancy application group

To display the redundancy group information, use the **show redundancy application group** command in privileged EXEC mode.

show redundancy application group [*group-id* | **all**]

Syntax Description

group-id	(Optional) redundancy group ID. Valid values are 1 and 2.
all	(Optional) Display the redundancy group information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

Use the **show redundancy application group** command to display the current state of each interbox redundancy group on the device and the peer device.

Examples

The following is sample output from the **show redundancy application group all** command:

```
Router# show redundancy application group all

Faults states Group 1 info:
        Runtime priority: [200]
                RG Faults RG State: Up.
                        Total # of switchovers due to faults:           3
                        Total # of down/up state changes due to faults: 2
Group ID:1
Group Name:grp2


Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: UNKNOWN
Peer Presence: No
Peer Comm: No
Peer Progression Started: No

RF Domain: btob-one
         RF state: ACTIVE
         Peer RF state: DISABLED


RG Protocol RG 1
------------------
        Role: Active
        Negotiation: Enabled
```

```
        Priority: 200
        Protocol state: Active
        Ctrl Intf(s) state: Down
        Active Peer: Local
        Standby Peer: Not exist
        Log counters:
                role change to active: 2
                role change to standby: 0
                disable events: rg down state 1, rg shut 0
                ctrl intf events: up 0, down 2, admin_down 1
                reload events: local request 3, peer request 0

RG Media Context for RG 1
--------------------------
        Ctx State: Active
        Protocol ID: 1
        Media type: Default
        Control Interface: GigabitEthernet0/1/0
        Hello timer: 5000
        Effective Hello timer: 5000, Effective Hold timer: 15000
         LAPT values: 0, 0
        Stats:
                Pkts 0, Bytes 0, HA Seq 0, Seq Number 0, Pkt Loss 0
                Authentication not configured
                Authentication Failure: 0
                Reload Peer: TX 0, RX 0
                Resign: TX 1, RX 0
        Standby Peer: Not Present.


Faults states Group 2 info:
        Runtime priority: [150]
                RG Faults RG State: Up.
                        Total # of switchovers due to faults:           2
                        Total # of down/up state changes due to faults: 2
Group ID:2
Group Name:name1

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: UNKNOWN
Peer Presence: No
Peer Comm: No
Peer Progression Started: No

RF Domain: btob-two
         RF state: ACTIVE
         Peer RF state: DISABLED


RG Protocol RG 2
-----------------
        Role: Active
        Negotiation: Enabled
        Priority: 150
        Protocol state: Active
        Ctrl Intf(s) state: Down
        Active Peer: Local
        Standby Peer: Not exist
        Log counters:
                role change to active: 1
                role change to standby: 0
                disable events: rg down state 1, rg shut 0
```

```
                ctrl intf events: up 0, down 2, admin_down 1
                reload events: local request 2, peer request 0

RG Media Context for RG 2
--------------------------
        Ctx State: Active
        Protocol ID: 2
        Media type: Default
        Control Interface: GigabitEthernet0/1/0
        Hello timer: 5000
        Effective Hello timer: 5000, Effective Hold timer: 15000
         LAPT values: 0, 0
        Stats:
                Pkts 0, Bytes 0, HA Seq 0, Seq Number 0, Pkt Loss 0
                Authentication not configured
                Authentication Failure: 0
                Reload Peer: TX 0, RX 0
                Resign: TX 0, RX 0
        Standby Peer: Not Present.
```

Table 183 describes the significant fields shown in the display.

Table 183 show redundancy application group all Field Descriptions

Field	Description
Faults states Group 1 info	Redundancy group faults information for Group 1.
Runtime priority	Current redundancy group priority of the group.
RG Faults RG State	Redundancy group state returned by redundancy group faults.
Total # of switchovers due to faults	Number of switchovers triggered by redundancy group fault events.
Total # of down/up state changes due to faults	Number of down and up state changes triggered by redundancy group fault events.
Group ID	Redundancy group ID.
Group Name	Redundancy group name.
Administrative State	The redundancy group state configured by users.
Aggregate operational state	Current redundancy group state.
My Role	The current role of the device.
Peer Role	The current role of the peer device.
Peer Presence	Indicates if the peer device is detected or not.
Peer Comm	Indicates the communication state with the peer device.
Peer Progression Started	Indicates if the peer box has started RF progression.
RF Domain	The name of RF domain for the redundancy group.

Related Commands

Command	Description
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application faults	Displays fault-specific information for a redundancy group.

Command	Description
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.
show redundancy application protocol	Displays protocol-specific information for a redundancy group.

show redundancy application if-mgr

To display interface manager information for a redundancy group, use the **show redundancy application if-mgr** command in privileged EXEC mode.

show redundancy application if-mgr group [*group-id*]

Syntax Description

group	Specifies the redundancy group.
group-id	(Optional) Redundancy group ID. Valid values are 1 to 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application if-mgr** command shows information of traffic interfaces protected by redundancy groups. When a traffic interface is functioning with the redundancy group, the state is no shut on the active device, and shut on the standby device. On the other hand, it is always shut on the standby device.

Examples

The following is sample output from the **show redundancy application if-mgr** command:

```
Router# show redundancy application if-mgr group 2

RG ID: 2
 Interface       VIP         VMAC        Shut   Decrement
 ============================================================
 GigabitEthernet0/1/7 10.1.1.3 0007.b422.0016  no shut    50
 GigabitEthernet0/3/1 11.1.1.3 0007.b422.0017  no shut    50
```

Table 184 describes the significant fields shown in the display.

Table 184 show redundancy application if-mgr Field Descriptions

Field	Description
RG ID	Redundancy group ID.
Interface	Interface name.
VIP	Virtual IP address for this traffic interface.
VMAC	Virtual MAC address for this traffic interface.

Table 184 show redundancy application if-mgr Field Descriptions (continued)

Field	Description
Shut	The state of this interface. **Note** It is always "shut" on the standby box.
Decrement	The decrement value for this interface. When this interface goes down, the runtime priority of its redundancy group decreases.

Related Commands

Command	Description
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application group	Displays redundancy group information.
show redundancy application protocol	Displays protocol-specific information for a redundancy group

show redundancy application protocol

To display protocol-specific information for a redundancy group, use the **show redundancy application protocol** command in privileged EXEC mode.

show redundancy application protocol {*protocol-id* | **group** [*group-id*]

Syntax Description

protocol-id	Protocol ID. The range is from 1 to 8.
group	Specifies the redundancy group.
group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application protocol** command shows information returned by redundancy group protocol.

Examples

The following is sample output from the **show redundancy application protocol** command:

```
Router# show redundancy application protocol 3

Protocol id: 3, name:
 BFD: ENABLE
 Hello timer in msecs: 0
 Hold timer in msecs: 0
```

Table 185 describes the significant fields shown in the display.

Table 185 show redundancy application protocol Field Descriptions

Field	Description
Protocol id	Redundancy group protocol ID.
BFD	Indicates whether the BFD protocol is enabled for the redundancy group protocol.
Hello timer in msecs	Redundancy group hello timer, in milliseconds, for the redundancy group protocol. The default is 3000 msecs.
Hold timer in msecs	Redundancy group hold timer, in milliseconds, for the redundancy group protocol. The default is 10000 msecs.

Related Commands

Command	Description
show redundancy application group	Displays redundancy group information.
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.

show redundancy application transport

To display transport-specific information for a redundancy group, use the **show redundancy application transport** command in privileged EXEC mode.

show redundancy application transport {**client** | **group** [*group-id*]}

Syntax Description

client	Displays transport client-specific information.
group	Displays the redundancy group name.
group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application transport** command shows information for redundancy group transport.

Examples

The following is sample output from the **show redundancy application transport group** command:

```
Router# show redundancy application transport group 1

Transport Information for RG (1)
```

Related Commands

Command	Description
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application group	Displays redundancy group information.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.
show redundancy application protocol	Displays protocol-specific information for a redundancy group.

show redundancy linecard-group

To display the components of a Blade Failure Group, use the **show redundancy linecard-group** command in privileged EXEC mode.

show redundancy linecard-group *group-id*

Syntax Description

group-id	Group ID.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example shows the components of a Blade Failure Group:

```
Router# show redundancy linecard-group 1
Line Card Redundancy Group:1 Mode:feature-card
Class:load-sharing
Cards:
Slot:3 Subslot:0
Slot:5 Subslot:0
```

Related Commands

Command	Description
linecard-group feature card	Assigns a group ID to a Blade Failure Group.

show running-config

To display the contents of the current running configuration file or the configuration for a specific module, Layer 2 VLAN, class map, interface, map class, policy map, or virtual circuit (VC) class, use the **show running-config** command in privileged EXEC mode.

show running-config [*options*]

Syntax Description

options	(Optional) Keywords used to customize output. You can enter more than one keyword. • **all**—Expands the output to include the commands that are configured with default parameters. If the **all** keyword is not used, the output does not display commands configured with default parameters. • **brief**—Displays the configuration without certification data and encrypted filter details. The **brief** keyword can be used with the **linenum** keyword. • **class-map** [*name*] [**linenum**]—Displays class map information. The **linenum** keyword can be used with the **class-map** *name* option. • **control-plane** [**cef-exception** | **host** | **transit**]—Displays control-plane information. The **cef-exception**, **host**, and **transit** keywords can be used with the **control-plane** option. • **flow** {**exporter** | **monitor** | **record**}—Displays global flow configuration commands. The **exporter**, **monitor**, and **record** keywords can be used with the **flow** option. • **full**—Displays the full configuration. • **interface** *type number*—Displays interface-specific configuration information. If you use the **interface** keyword, you must specify the interface type and the interface number (for example, **interface ethernet 0**). Keywords for common interfaces include **async**, **ethernet**, **fastEthernet**, **group-async**, **loopback**, **null**, **serial**, and **virtual-template**. Use the **show run interface ?** command to determine the interfaces available on your system. • **linenum**—Displays line numbers in the output. The **brief** or **full** keyword can be used with the **linenum** keyword. The **linenum** keyword can be used with the **class-map**, **interface**, **map-class**, **policy-map**, and **vc-class** keywords. • **map-class** [**atm** | **dialer** | **frame-relay**] [**name**] [**linenum**]—Displays map class information. This option is described separately; see the **show running-config map-class** command page.

- **partition types**—Displays the configuration corresponding to a partition. The **types** keyword can be used with the **partition** option.
- **policy-map** [*name*] [**linenum**]—Displays policy map information. The **linenum** keyword can be used with the **policy-map** *name* option.
- **vc-class** [*name*] [**linenum**]—Displays VC-class information (the display is available only on certain routers such as the Cisco 7500 series routers). The **linenum** keyword can be used with the **vc-class** *name* option.
- **view full**—Enables the display of a full running configuration. This is for view-based users who typically can only view the configuration commands that they are entitled to access for that particular view.
- **vrf** *name*—Displays the Virtual routing and forwarding (VRF)-aware configuration module number.
- **vlan** [*vlan-id*]—Displays the specific VLAN information ; valid values are from 1 to 4094.

Command Default

The default syntax, **show running-config**, displays the contents of the running configuration file, except commands configured using the default parameters.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.0	This command was replaced by the **more system:running-config** command.
12.0(1)T	This command was integrated into Cisco IOS Release 12.0(1)T, and the output modifier (|) was added.
12.2(4)T	This command was modified. The **linenum** keyword was added.
12.3(8)T	This command was modified. The **view full** option was added.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX. The **module** *number* and **vlan** *vlan-id* keywords and arguments were added for the Supervisor Engine 720.
12.2(17d)SXB	This command was integrated into Release 12.2(17d)SXB and implemented on the Supervisor Engine 2.
12.2(33)SXH	This command was modified. The **all** keyword was added.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command was enhanced to display the configuration information for traffic shaping overhead accounting for ATM and was implemented on the Cisco 10000 series router for the PRE3.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was modified. Support for the Cisco 7300 series router was added.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **partition** and **vrf** keywords were added. The **module** and **vlan** keywords were removed.

15.0(1)M	This command was modified. The output was modified to include encrypted filter information.
12.2(33)SXI	This command was modified. The output was modified to display Access Control List (ACL) information.

Usage Guidelines

The **show running-config** command is technically a command alias (substitute or replacement syntax) of the **more system:running-config** command. Although the use of more commands is recommended (because of their uniform structure across platforms and their expandable syntax), the **show running-config** command remains enabled to accommodate its widespread use, and to allow typing shortcuts such as **show run**.

The **show running-config interface** command is useful when there are multiple interfaces and you want to look at the configuration of a specific interface.

The **linenum** keyword causes line numbers to be displayed in the output. This option is useful for identifying a particular portion of a very large configuration.

You can enter additional output modifiers in the command syntax by including a pipe character (|) after the optional keyword. For example, **show running-config interface serial 2/1 linenum | begin 3**. To display the output modifiers that are available for a keyword, enter **| ?** after the keyword. Depending on the platform you are using, the keywords and the arguments for the *options* argument may vary.

Prior to Cisco IOS Release 12.2(33)SXH, the **show running-config** command output omitted configuration commands set with default values. Effective with Cisco IOS Release 12.2(33)SXH, the **show running-config all** command displays complete configuration information, including the default settings and values. For example, if the Cisco Discovery Protocol (abbreviated as CDP in the output) hold-time value is set to its default of 180:

- The **show running-config** command does not display this value.
- The **show running-config all** displays the following output: `cdp holdtime 180.`

If the Cisco Discovery Protocol holdtime is changed to a nondefault value (for example, 100), the output of the **show running-config** and **show running-config all** commands is the same; that is, the configured parameter is displayed.

Note In Cisco IOS Release 12.2(33)SXH, the **all** keyword expands the output to include some of the commands that are configured with default values. In subsequent Cisco IOS releases, additional configuration commands that are configured with default values will be added to the output of the **show running-config all** command.

Effective with Cisco IOS Release 12.2(33)SXI, the **show running-config** command displays ACL information. To exclude ACL information from the output, use the **show running | section exclude ip access | access list** command.

Cisco 7600 Series Router

In some cases, you might see a difference in the duplex mode that is displayed between the **show interfaces** command and the **show running-config** command. The duplex mode that is displayed in the **show interfaces** command is the actual duplex mode that the interface is running. The **show interfaces** command displays the operating mode of an interface, and the **show running-config** command displays the configured mode of the interface.

The **show running-config** command output for an interface might display the duplex mode but no configuration for the speed. This output indicates that the interface speed is configured as auto and that the duplex mode that is displayed becomes the operational setting once the speed is configured to something other than auto. With this configuration, it is possible that the operating duplex mode for that interface does not match the duplex mode that is displayed with the **show running-config** command.

Examples

The following example shows the configuration for serial interface 1. The fields are self-explanatory.

```
Router# show running-config interface serial 1

Building configuration...

Current configuration:
!
interface Serial1
 no ip address
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 shutdown
end
```

The following example shows the configuration for Ethernet interface 0/0. Line numbers are displayed in the output. The fields are self-explanatory.

```
Router# show running-config interface ethernet 0/0 linenum

Building configuration...

Current configuration : 104 bytes
 1 : !
 2 : interface Ethernet0/0
 3 :  ip address 10.4.2.63 255.255.255.0
 4 :  no ip route-cache
 5 :  no ip mroute-cache
 6 : end
```

The following example shows how to set line numbers in the command output and then use the output modifier to start the display at line 10. The fields are self-explanatory.

```
Router# show running-config linenum | begin 10

   10 : boot-start-marker
   11 : boot-end-marker
   12 : !
   13 : no logging buffered
   14 : enable password #####
   15 : !
   16 : spe 1/0 1/7
   17 :  firmware location bootflash:mica-modem-pw.172.16.0.0.bin
   18 : !
   19 : !
   20 : resource-pool disable
   21 : !
   22 : no aaa new-model
   23 : ip subnet-zero
   24 : ip domain name cisco.com
   25 : ip name-server 172.16.11.48
   26 : ip name-server 172.16.2.133
   27 : !
   28 : !
```

```
   29 : isdn switch-type primary-5ess
   30 : !
   .
   .
   .
   126 : end
```

The following example shows how to display the module and status configuration for all modules on a Cisco 7600 series router. The fields are self-explanatory.

```
Router# show running-config

Building configuration...

Current configuration:
!
version 12.0
service timestamps debug datetime localtime
service timestamps log datetime localtime
no service password-encryption
!
hostname Router
!
boot buffersize 126968
boot system flash slot0:7600r
boot bootldr bootflash:c6msfc-boot-mz.120-6.5T.XE1.0.83.bin
enable password lab
!
clock timezone Pacific -8
clock summer-time Daylight recurring
redundancy
 main-cpu
  auto-sync standard
!
ip subnet-zero
!
ip multicast-routing
ip dvmrp route-limit 20000
ip cef
mls flow ip destination
mls flow ipx destination
cns event-service server
!
spanning-tree portfast bpdu-guard
spanning-tree uplinkfast
spanning-tree vlan 200 forward-time 21
port-channel load-balance sdip
!
!
!
 shutdown
!
!
.
.
.
```

In the following sample output from the **show running-config** command, the **shape average** command indicates that the traffic shaping overhead accounting for ATM is enabled. The BRAS-DSLAM encapsulation type is qinq and the subscriber line encapsulation type is snap-rbe based on the ATM adaptation layer 5 (AAL5) service. The fields are self-explanatory

```
Router# show running-config
.
.
.
subscriber policy recording rules limit 64
no mpls traffic-eng auto-bw timers frequency 0
call rsvp-sync
!
controller T1 2/0
    framing sf
    linecode ami
!
controller T1 2/1
    framing sf
    linecode ami
!
!
policy-map unit-test
    class class-default
        shape average percent 10 account qinq aal5 snap-rbe
!
```

The following is sample output from the **show running-config class-map** command. The fields in the display are self-explanatory.

```
Router# show running-config class-map

Building configuration...

Current configuration : 2910 bytes
!
class-map type stack match-all ip_tcp_stack
 match field IP protocol eq 0x6 next TCP
class-map type access-control match-all my
 match field UDP dest-port eq 1111
 match encrypted
  filter-version 0.1, Dummy Filter 2
  filter-id      123
  filter-hash    DE0EB7D3C4AFDD990038174A472E4789
  algorithm      aes256cbc
  cipherkey      realm-cisco.sym
  ciphervalue    #
oeahb4L6JK+XuC0q8k9AqXvBeQWzVfdg8WV67WEXbiWdXGQs6BEXqQeb4Pfow570zM4eDw0gxlp/Er8w
/lXsmolSgYpYuxFMYb1KX/H2iCXvA76VX7w5TE1b/+6ekgbfP/d5ms6DEzKa8DlOpl+Q95lP194PsIlU
wCyfVCwLS+T8p3RDLi8dKBgQMcDW4Dha1ObBJTpV4zpwhEdMvJDu5PATtEQhFjhN/UYeyQiPRthjbkJn
LzT8hQFxwYwVW8PCjkyqEwYrr+R+mFG/C7tFRiooaW9MU9PCpFd95FARvlU=#
  exit
class-map type stack match-all ip_udp_stack
 match field IP protocol eq 0x11 next UDP
class-map type access-control match-all psirt1
 match encrypted
  filter-version 0.0_DummyVersion_20090101_1830
  filter-id      cisco-sa-20090101-dummy_ddts_001
  filter-hash    FC50BED10521002B8A170F29AF059C53
  algorithm      aes256cbc
  cipherkey      realm-cisco.sym
  ciphervalue    #
DkGbVq0FPAsVJKguU15lQPDfZyTcHUXWsj8+tD+dCSYW9cjkRU9jyST4vO4u69/L62QlbyQuKdyQmb10
6sAeY5vDsDfDV05k4o5eD+j8cMt78iZT0Qg7uGiBSYBbak3kKn/5w2gDd1vnivyQ7g4Ltd9+XM+GP6XL
27RrXeP5A5iGbzC7KI9t6riZXk0gmR/vFw1a5wck0D/iQHIlFa/yRPoKMSFlqfIlLTe5NM7JArSTKET2
pu7wZammTz4FF6rY#
  exit
 match start TCP payload-start offset 0 size 10 regex "abc.*def"
 match field TCP source-port eq 1234
```

```
class-map type access-control match-all psirt2
 match encrypted
  filter-version 0.0_DummyVersion_20090711_1830
  filter-id      cisco-sa-20090711-dummy_ddts_002
  filter-hash    DE0EB7D3C4AFDD990038174A472E4789
  algorithm      aes256cbc
  cipherkey      realm-cisco.sym
```

Related Commands

Command	Description
bandwidth	Specifies or modifies the bandwidth allocated for a class belonging to a policy map, and enables ATM overhead accounting.
boot config	Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).
configure terminal	Enters global configuration mode.
copy running-config startup-config	Copies the running configuration to the startup configuration. (Command alias for the **copy system:running-config nvram:startup-config** command.)
shape	Shapes traffic to the indicated bit rate according to the algorithm specified, and enables ATM overhead accounting.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps, and displays ATM overhead accounting information, if configured.
show startup-config	Displays the contents of NVRAM (if present and valid) or displays the configuration file pointed to by the CONFIG_FILE environment variable. (Command alias for the **more:nvram startup-config** command.)

show running-config vrf

To display the subset of the running configuration of a router that is linked to a specific Virtual Private Network (VPN) routing and forwarding (VRF) instance or to all VRFs configured on the router, use the **show running-config vrf** command in user EXEC or privileged EXEC mode.

show running-config vrf [*vrf-name*]

Syntax Description

vrf-name	(Optional) Name of the VRF configuration that you want to display.

Command Default

If you do not specify a *vrf-name* argument, the running configurations of all VRFs on the router are displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **show running-config vrf** command to display a specific VRF configuration or to display all VRF configurations on the router. To display the configuration of a specific VRF, enter the name of the VRF as an argument to the command.

This command displays the following elements of the VRF configuration:

- The VRF submode configuration
- The routing protocol and static routing configurations associated with the VRF
- The configuration of the interfaces in the VRF, which includes the configuration of any owning controller and physical interface for a subinterface

Examples

The following is sample output from the **show running-config vrf** command. It includes a base VRF configuration for VRF vpn3 and Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF) configurations associated with VRF vpn3.

```
Router# show running-config vrf vpn3

Building configuration...

Current configuration : 604 bytes
ip vrf vpn3
 rd 100:3
```

```
 route-target export 100:3
 route-target import 100:3
!
!
interface Loopback1
 ip vrf forwarding vpn3
 ip address 10.43.43.43 255.255.255.255
!
interface Ethernet6/0
 ip vrf forwarding vpn3
 ip address 172.17.0.1 255.0.0.0
 no ip redirects
 duplex half
!
router bgp 100
!
address-family ipv4 vrf vpn3
 redistribute connected
 redistribute ospf 101 match external 1 external 2
 no auto-summary
 no synchronization
 exit-address-family
 !
router ospf 101 vrf vpn3
 log-adjacency-changes
 area 1 sham-link 10.43.43.43 10.23.23.23 cost 10
 network 172.17.0.0 0.255.255.255 area 1
!
end
```

Table 186 describes the significant fields shown in the display.

Table 186 show running-config vrf Field Descriptions

Field	Description
Current configuration: 604 bytes	Number of bytes (604) in the VRF vpn3 configuration.
ip vrf vpn3	Name of the VRF (vpn3) for which the configuration is displayed.
rd 100:3	Identifies the route distinguisher (100:3) for VRF vpn3.
route-target export 100:3 route-target import 100:3	Specifies the route-target extended community for VRF vpn3. • Routes tagged with route-target export 100:3 are exported from VRF vpn3. • Routes tagged with the route-target import 100:3 are imported into VRF vpn3.
interface Loopback1	Virtual interface associated with VRF vpn3.
ip vrf forwarding vpn3	Associates VRF vpn3 with the named interface.
ip address 10.43.43.43 255.255.255.255	IP address of the loopback interface.
interface Ethernet6/0	Interface associated with VRF vpn3.
ip address 172.17.0.1 255.0.0.0	IP address of the Ethernet interface.

Table 186 show running-config vrf Field Descriptions (continued)

Field	Description
router bgp 100	Sets up a BGP routing process for the router with autonomous system number 100.
address-family ipv4 vrf vpn3	Sets up a routing session for VRF vpn3 using standard IP Version 4 address prefixes.
redistribute connected	Redistributes routes automatically established by IP on an interface into the BGP routing domain.
redistribute ospf 101 match external 1 external 2	Redistribute routes from the OSPF 101 routing domain into the BGP routing domain.
router ospf 101 vrf vpn3	Set up an OSPF routing process and associates VRF vpn3 with OSPF VRF processes.
area 1 sham-link 10.43.43.43 10.23.23.23 cost 10	Configure a sham-link interface on a provider edge (PE) router in a Multiprotocol Label Switching (MPLS) VPN backbone. • 1 is the ID number of the OSPF area assigned to the sham-link. • 10.43.43.43 is the IP address of the source PE router. • 10.23.23.23 is the IP address of the destination PE router. • 10 is the OSPF cost to send IP packets over the sham-link interface.
network 172.17.0.0 0.255.255.255 area 1	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.

Related Commands

Command	Description
ip vrf	Configures a VRF routing table.
show ip interface	Displays the usability status of interfaces configured for IP.
show ip vrf	Displays the set of defined VRFs and associated interfaces.
show running-config interface	Displays the configuration for a specific interface.

show sasl

To display Simple Authentication and Security Layer (SASL) information, use the **show sasl** command in user EXEC or privileged EXEC mode.

show sasl {**all** | **context** | **mechanisms** | **profile** {*profile-name* | **all**}}

Syntax Description

all	Displays detailed information for all SASL profiles.
context	Displays context information for SASL profiles.
mechanisms	Displays the mechanisms applied for all SASL profiles.
profile *profile-name*	Displays detailed information for the specified SASL profile.
profile all	Displays all configured profiles.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following is sample output from the **show sasl profile all** command:

```
Router# show sasl profile all

SASL profile 'sgw_sasl' Refs:0 Mechs:0x2
    client:  <NONE>/<NONE>
    servers: ravi/ravi

SASL profile 'sgw_1' Refs:0 Mechs:0x1
    client:  us1/pw1
    servers: server1/user
```

Table 187 describes the significant fields shown in the display.

Table 187 show sasl profile all Field Descriptions

Field	Description
SASL profile	Indicates the name of the SASL profile.
Refs	Indicates the number of active sessions.
Mechs	Indicates the profile mechanisms configured.

Table 187 show sasl profile all Field Descriptions (continued)

Field	Description
client	Indicates the SASL client configured for the specified profile.
servers	Indicates the SASL server configured for the specified profile.

Related Commands

Command	Description
sasl	Configures SASL.

show secure bootset

To display the status of Cisco IOS image and configuration resilience, use the **show secure** command in privileged EXEC mode.

show secure bootset

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the **show secure bootset** command, instead of the Cisco IOS directory listing **dir** command, to verify the existence of an image archive. This command also displays output that specifies whether the image or configuration archive is ready for an upgrade.

Examples

The following is sample output from the **show secure bootset** command. The field descriptions are self-explanatory:

```
Router# show secure bootset

%IOS image and configuration resilience is not active


Router# show secure bootset

IOS resilience router id JMX0704L5GH

IOS image resilience version 12.3 activated at 08:16:51 UTC Sun Jun 16 2002
Secure archive slot0:c3745-js2-mz type is image (elf) []
  file size is 25469248 bytes, run size is 25634900 bytes
  Runnable image, entry point 0x80008000, run from ram

IOS configuration resilience version 12.3 activated at 08:17:02 UTC Sun Jun 16 2002
Secure archive slot0:.runcfg-20020616-081702.ar type is config
configuration archive size 1059 bytes
```

Related Commands

Command	Description
dir	Displays a list of files on a file system.
secure boot-config	Saves a secure copy of the router running configuration in persistent storage.
secure boot-image	Enables Cisco IOS image resilience.

show smm

To display string matching module (SMM) information, use the **show smm** command in privileged EXEC mode.

show smm {**counters** | **timing** | **tree** [*tree-index* | **details**]}

Syntax Description

counters	Displays information about SMM counters.
timing	Displays timing information about the SMM.
tree	Displays the AVL tree containing the string information.
tree-index	(Optional) Specifies the tree index.
details	(Optional) Displays detailed information about the AVL tree.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)	This command was introduced in a release earlier than Cisco IOS Release 15.0(1) on Cisco 3845 series routers.

Examples

The following is sample output from the **show smm counters** command. Fields in the output are self-explanatory.

```
Router# show smm counters

Number of non-matching packets processed   - 0
Number of cache hits                       - 0
Number of cache misses                     - 0
Cache full instances                       - 0

Number of matching packets processed       - 0

Number of matches for Stage0               - 0
Number of matches for Stage1               - 0
Number of matches for Stage2               - 0
Number of matches for Stage3               - 0

Number of signatures in signature database - 0
```

The following is sample output from the **show smm timing** command:

```
Router# show smm timing

Packet processing stats (in microseconds) :
-------------------------------------------
Minimum processing time per packet - 0
Maximum processing time per packet - 0
Average processing time for non-matching packets - 0
Average processing time for matching packets     - 0
```

Related Commands

Command	Description
action string match	Returns 1 to the $_string_result, if the string matches the pattern when an EEM applet is triggered.

show snmp mib nhrp status

To display status information about the Next Hop Resolution Protocol (NHRP) MIB, use the **show snmp mib nhrp status** command in privileged EXEC mode.

show snmp mib nhrp status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

This command is used to display the status of the MIB for NHRP and whether the NHRP MIB is enabled or disabled.

Examples

The following output is from the **show snmp mib nhrp status** command:

```
Spoke_103# show snmp mib nhrp status

NHRP-SNMP Agent Feature: Enabled
NHRP-SNMP Tree State: Good
ListEnqueue Count = 0 Node Malloc Counts = 1
Spoke_103#
```

Table 1 describes the significant fields shown in the display.

Table 188 show snmp mib nhrp status Field Descriptions

Field	Description
NHRP-SNMP Agent Feature:	Shows the status of the NHRP MIB. “Enabled” indicates that the NHRP MIB is enabled. If the NHRP MIB was disabled, it would display “Disabled”.
ListEnqueue Count	Indicates how many nodes have been queued for freeing.
Node Malloc Counts	Indicates how many nodes are allocated.

Related Commands

Command	Description
show snmp mib	Displays a list of the MIB OIDs registered on the system.

show ssh

To display the status of Secure Shell (SSH) server connections on the router, use the **show ssh** command in user EXEC or privileged EXEC mode.

show ssh vty [*ssh-number*]

Syntax Description

vty	Displays virtual terminal line (VTY) connection details.
ssh-number	(Optional) The number of SSH server connections on the router. Range is from 0 to 1510. The default value is 0.

Command Modes

User Exec (>)
Privileged EXEC (#)

Command History

Release	Modification
12.1(15)T	This command was introduced.
12.2(33)SRA	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was modified. It was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use the **show ssh** command to display the status of the SSH connections on your router. This command does not display any SSH configuration data. Use the **show ip ssh** command for SSH configuration information such as timeouts and retries.

Examples

The following is sample output from the **show ssh** command with SSH enabled:

```
Router# show ssh

Connection     Version      Encryption     State                Username
0               1.5         3DES           Session Started       guest
```

Table 189 describes the significant fields shown in the display.

Table 189 show ssh Field Descriptions

Field	Description
Connection	Number of SSH connections on the router.
Version	Version number of the SSH terminal.
Encryption	Type of transport encryption.

Table 189 show ssh Field Descriptions (continued)

Field	Description
State	The status of SSH connection to indicate if the session has started or stopped.
Username	Uesrname to log in to the SSH.

Related Commands

Command	Description
show ip ssh	Displays version and configuration data for SSH.

show ssl-proxy module state

To display the spanning-tree state for the specified VLAN, enter the **show ssl-proxy module state** command in EXEC mode.

show ssl-proxy module *mod* **state**

Syntax Description		
	mod	Module number.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Secure Sockets Layer (SSL) Services Module only.

Examples

This example shows how to verify that the VLAN information displayed matches the VLAN configuration:

```
Router# show ssl-proxy module 6 state

SSL-services module 6 data-port:
 Switchport:Enabled
Administrative Mode:trunk
Operational Mode:trunk
Administrative Trunking Encapsulation:dot1q
Operational Trunking Encapsulation:dot1q
Negotiation of Trunking:Off
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Trunking VLANs Enabled:100
Pruning VLANs Enabled:2-1001
Vlans allowed on trunk:100
Vlans allowed and active in management domain:100
Vlans in spanning tree forwarding state and not pruned:
100
Allowed-vlan :100
Router#
```

Related Commands

Command	Description
ssl-proxy module allowed-vlan	Adds the VLANs allowed over the trunk to the SSL Services Module.

show tacacs

To display statistics for a TACACS+ server, use the **show tacacs** command in privileged EXEC mode.

show tacacs [**private | public**]

Syntax Description

private	(Optional) Displays private tacacs+ server statistics.
public	(Optional) Displays public tacacs+ server statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3. The **private** and **public** keywords were added.

Examples

The following example is sample output for the **show tacacs** command:

```
Router# show tacacs

Tacacs+ Server            : 172.19.192.80/49
              Socket opens:          3
             Socket closes:          3
             Socket aborts:          0
             Socket errors:          0
          Socket Timeouts:           0
   Failed Connect Attempts:          0
        Total Packets Sent:          7
        Total Packets Recv:          7
          Expected Replies:          0
  No current connection
```

he following is sample output from the **show tacacs** command for the private IP address 192.168.0.0:

```
Router# show tacacs private 192.168.0.0

Tacacs+ Server -  private  :  192.168.0.0
              Socket opens:          0
             Socket closes:          0
             Socket aborts:          0
             Socket errors:          0
          Socket Timeouts:           0
   Failed Connect Attempts:          0
        Total Packets Sent:          0
        Total Packets Recv:          0
```

The following is sample output from the **show tacacs** command for the public IP address 209.165.200.224:

```
Router# show tacacs public 209.165.200.224

Tacacs+ Server -  public  :  209.165.200.224
              Socket opens:          0
             Socket closes:          0
             Socket aborts:          0
             Socket errors:          0
          Socket Timeouts:           0
   Failed Connect Attempts:          0
        Total Packets Sent:          0
        Total Packets Recv:          0
```

Table 190 describes the significant fields shown in the display.

Table 190 show tacacs Field Descriptions

Field	Description
Tacacs+ Server	IP address of the TACACS+ server.
Socket opens	Number of successful TCP socket connections to the TACACS+ server.
Socket closes	Number of successfully closed TCP socket attempts.
Socket aborts	Number of premature TCP socket closures to the TACACS+ server; That is, the peer did not wait for a reply from the server after a the peer sent its request.
Socket errors	Any other socket read or write errors, such as incorrect packet format and length.
Failed Connect Attempts	Number of failed TCP socket connections to the TACACS+ server.
Total Packets Sent	Number of packets sent to the TACACS+ server.
Total Packets Recv	Number of packets received from the TACACS+ server.
Tacacs+ Server	IP address of the TACACS+ server.

Related Commands

Command	Description
tacacs-server host	Specifies a TACACS+ host.

show tcp intercept connections

To display TCP incomplete and established connections, use the **show tcp intercept connections** command in EXEC mode.

show tcp intercept connections

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show tcp intercept connections** command to display TCP incomplete and established connections.

Examples

The following is sample output from the **show tcp intercept connections** command:

```
Router# show tcp intercept connections

Incomplete:
Client                Server                State    Create   Timeout  Mode
172.19.160.17:58190   10.1.1.30:23          SYNRCVD  00:00:09 00:00:05 I
172.19.160.17:57934   10.1.1.30:23          SYNRCVD  00:00:09 00:00:05 I

Established:
Client                Server                State    Create   Timeout  Mode
172.16.232.23:1045    10.1.1.30:23          ESTAB    00:00:08 23:59:54 I
```

Table 191 describes significant fields shown in the display.

Table 191 show tcp intercept connections Field Descriptions

Field	Description
Incomplete:	Rows of information under “Incomplete” indicate connections that are not yet established.
Client	IP address and port of the client.
Server	IP address and port of the server being protected by TCP intercept.

Table 191 show tcp intercept connections Field Descriptions (continued)

Field	Description
State	SYNRCVD—establishing with client. SYNSENT—establishing with server. ESTAB—established with both, passing data.
Create	Hours:minutes:seconds since the connection was created.
Timeout	Hours:minutes:seconds until the retransmission timeout.
Mode	I—intercept mode. W—watch mode.
Established:	Rows of information under "Established" indicate connections that are established. The fields are the same as those under "Incomplete" except for the Timeout field described below.
Timeout	Hours:minutes:seconds until the connection will timeout, unless the software sees a FIN exchange, in which case this indicates the hours:minutes:seconds until the FIN or RESET timeout.

Related Commands

Command	Description
ip tcp intercept connection-timeout	Changes how long a TCP connection will be managed by the TCP intercept after no activity.
ip tcp intercept finrst-timeout	Changes how long after receipt of a reset or FIN-exchange the software ceases to manage the connection.
ip tcp intercept list	Enables TCP intercept.
show tcp intercept statistics	Displays TCP intercept statistics.

show tcp intercept statistics

To display TCP intercept statistics, use the **show tcp intercept statistics** command in EXEC mode.

show tcp intercept statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show tcp intercept statistics** command to display TCP intercept statistics.

Examples

The following is sample output from the **show tcp intercept statistics** command:

```
Router# show tcp intercept statistics

intercepting new connections using access-list 101
2 incomplete, 1 established connections (total 3)
1 minute connection request rate 2 requests/sec
```

Related Commands

Command	Description
ip tcp intercept connection-timeout	Changes how long a TCP connection will be managed by the TCP intercept after no activity.
ip tcp intercept finrst-timeout	Changes how long after receipt of a reset or FIN-exchange the software ceases to manage the connection.
ip tcp intercept list	Enables TCP intercept.
show tcp intercept connections	Displays TCP incomplete and established connections.

show tech-support

To display general information about the router when it reports a problem, use the **show tech-support** command in privileged EXEC mode.

show tech-support [**page**] [**password**] [**cef** | **ipc** | **ipmulticast** [**vrf** *vrf-name*] | **isis** | **mpls** | **ospf** [*process-id* | **detail**] | **rsvp** | **voice** | **wccp**]

Cisco 7600 Series

show tech-support [**cef** | **ipmulticast** [**vrf** *vrf-name*] | **isis** | **password** [**page**] | **platform** | **page** | **rsvp**]

Syntax Description

page	(Optional) Causes the output to display a page of information at a time.
password	(Optional) Leaves passwords and other security information in the output.
cef	(Optional) Displays **show** command output specific to Cisco Express Forwarding.
ipc	(Optional) Displays **show** command output specific to Inter-Process Communication (IPC).
ipmulticast	(Optional) Displays **show** command output related to the IP Multicast configuration, including Protocol Independent Multicast (PIM) information, Internet Group Management Protocol (IGMP) information, and Distance Vector Multicast Routing Protocol (DVMRP) information.
vrf *vrf-name*	(Optional) Specifies a multicast Virtual Private Network (VPN) routing and forwarding instance (VRF).
isis	(Optional) Displays **show** command output specific to Connectionless Network Service (CLNS) and Intermediate System-to-Intermediate System Protocol (IS-IS).
mpls	(Optional) Displays **show** command output specific to Multiprotocol Label Switching (MPLS) forwarding and applications.
ospf [*process-id* | **detail**]	(Optional) Displays **show** command output specific to Open Shortest Path First Protocol (OSPF) networking.
rsvp	(Optional) Displays **show** command output specific to Resource Reservation Protocol (RSVP) networking.
voice	(Optional) Displays **show** command output specific to voice networking.
wccp	(Optional) Displays **show** command output specific to Web Cache Communication Protocol (WCCP).
platform	(Optional) Displays platform-specific **show** command output.

Defaults

The output scrolls without page breaks.
Passwords and other security information are removed from the output.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2	This command was introduced.
11.3(7), 11.2(16)	The output for this command was expanded to show additional information for **boot**, **bootflash**, **context**, and **traffic** for all enabled protocols.
12.0	The output for this command was expanded to show additional information for **boot**, **bootflash**, **context**, and **traffic** for all enabled protocols. The **cef**, **ipmulticast**, **isis**, **mlps**, and **ospf** keywords were added to this command.
12.2(13)T	Support for AppleTalk EIGRP, Apollo Domain, Banyan VINES, Novell Link-State Protocol, and XNS was removed from Cisco IOS software.
12.2(14)SX	Support for this command was added for the Supervisor Engine 720.
12.3(4)T	The output of this command was expanded to include the output from the **show inventory** command.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(30)S	The **show tech-support ipmulticast** command was changed as follows: • Support for bidirectional PIM and Multicast VPN (MVPN) was added. CSCeh94431 • The **vrf** *vrf-name* option was added. CSCeh94431 The output of the **show tech-support ipmulticast** command (without the **vrf** *vrf-name* keyword and argument) was changed to include the output from these commands: • **show ip pim int df** • **show ip pim mdt** • **show ip pim mdt bgp** • **show ip pim rp metric**
12.3(16)	This command was integrated into Cisco IOS Release 12.3(16).
12.2(18)SXF	The **show tech-support ipmulticast** command was changed as follows: • Support for bidirectional PIM and MVPN was added. CSCeh94431 • The **vrf** *vrf-name* option was added. CSCeh94431 The output of the **show tech-support ipmulticast vrf** command was changed to include the output from these commands: CSCeh87476 • **show mls ip multicast rp-mapping gm-cache** • **show mmls gc process** • **show mmls msc rpdf-cache** The output of the **show tech-support ipmulticast** command (without the **vrf** *vrf-name* keyword and argument) was changed to include the output from these commands: • **show ip pim int df** • **show ip pim mdt** • **show ip pim mdt bgp** • **show ip pim rp metric** Support to interrupt and terminate the **show tech-support** output was added.

Release	Modification
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.4(7)	This command was integrated into Cisco IOS Release 12.4(7).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(9)T	The output of this command was expanded to include partial **show dmvpn details** command output.
15.0(1)M	This command was modified. The **wccp** and **voice** keywords were added.
12.2(33)SRE	This command was modified. The **wccp** keyword was added.
Cisco IOS XE Release 2.5	This command was modified. The **wccp** keyword was added.

Usage Guidelines

To interrupt and terminate the **show tech-support** output, simultaneously press and release the **CTRL**, **ALT**, and **6** keys.

Press the **Return** key to display the next line of output, or press the **Spacebar** to display the next page of information. If you do not enter the **page** keyword, the output scrolls (that is, it does not stop for page breaks).

If you do not enter the **password** keyword, passwords and other security-sensitive information in the output are replaced with the label "<removed>."

The **show tech-support** command is useful for collecting a large amount of information about your routing device for troubleshooting purposes. The output of this command can be provided to technical support representatives when reporting a problem.

Note This command can generate a very large amount of output. You may want to redirect the output to a file using the **show inventory | redirect** *url* command syntax extension. Redirecting the output to a file also makes sending this output to your technical support representative easier. See the command documentation for **show <command> | redirect** for more information on this option.

The **show tech-support** command displays the output of a number of **show** commands at once. The output from this command varies depending on your platform and configuration. For example, access servers display voice-related **show** command output. Additionally, the **show** *protocol* **traffic** commands are displayed for only the protocols enabled on your device. For a sample display of the output of the **show tech-support** command, see the individual **show** command listed.

If you enter the **show tech-support** command without arguments, the output displays, but is not limited to, the equivalent of these **show** commands:

- **show appletalk traffic**
- **show bootflash**
- **show bootvar**
- **show buffers**
- **show cdp neighbors**
- **show cef**
- **show clns traffic**
- **show context**
- **show controllers**

- **show decnet traffic**
- **show disk0: all**
- **show dmvpn details**
- **show environment**
- **show fabric channel-counters**
- **show file systems**
- **show interfaces**
- **show interfaces switchport**
- **show interfaces trunk**
- **show ip interface**
- **show ip traffic**
- **show logging**
- **show mac-address-table**
- **show module**
- **show power**
- **show processes cpu**
- **show processes memory**
- **show running-config**
- **show spanning-tree**
- **show stacks**
- **show version**
- **show vlan**

Note Crypto information is not duplicated by the **show dmvpn details** command output.

When the **show tech-support** command is entered on a virtual switch (VS), the output displays the output of the **show module** command and the **show power** command for both the active and standby switches.

Use of the optional **cef**, **ipc**, **ipmulticast**, **isis**, **mpls**, **ospf**, or **rsvp** keywords provides a way to display a number of **show** commands specific to a particular protocol or process in addition to the **show** commands listed previously.

For example, if your Technical Assistance Center (TAC) support representative suspects that you may have a problem in your Cisco Express Forwarding (CEF) configuration, you may be asked to provide the output of the **show tech-support cef** command. The **show tech-support** [**page**] [**password**] **cef** command will display the output from the following commands in addition to the output for the standard **show tech-support** command:

- **show adjacency summary**
- **show cef drop**
- **show cef events**
- **show cef interface**

- **show cef not-cef-switched**
- **show cef timers**
- **show interfaces stats**
- **show ip cef events summary**
- **show ip cef inconsistency records detail**
- **show ip cef summary**

If you enter the **ipmulticast** keyword, the output displays, but is not limited to, these **show** commands:

- **show ip dvmrp route**
- **show ip igmp groups**
- **show ip igmp interface**
- **show ip mcache**
- **show ip mroute**
- **show ip mroute count**
- **show ip pim interface**
- **show ip pim interface count**
- **show ip pim interface df**
- **show ip pim mdt**
- **show ip pim mdt bgp**
- **show ip pim neighbor**
- **show ip pim rp**
- **show ip pim rp metric**
- **show mls ip multicast rp-mapping gm-cache**
- **show mmls gc process**
- **show mmls msc rpdf-cache**

If you enter the **wccp** keyword, the output displays, but is not limited to, these **show** commands:

- **show ip wccp** *service-number*
- **show ip wccp interfaces cef**

Examples

For a sample display of the output from the **show tech-support** command, refer to the documentation for the **show** commands listed in the "Usage Guidelines" section.

Related Commands

Command	Description
dir	Displays a list of files on a file system.
show appletalk traffic	Displays statistics about AppleTalk traffic, including MAC IP traffic.
show bootflash	Displays the contents of boot flash memory.

Command	Description
show bootvar	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.
show buffers	Displays statistics for the buffer pools on the network server.
show cdp neighbors	Displays detailed information about neighboring devices discovered using Cisco Discovery Protocol.
show cef	Displays information about packets forwarded by Cisco Express Forwarding.
show clns traffic	Displays a list of the CLNS packets this router has seen.
show <*command*> **| redirect**	Redirects the output of any **show** command to a file.
show context	Displays context data.
show controllers	Displays information that is specific to the hardware.
show controllers tech-support	Displays general information about a VIP card for problem reporting.
show decnet traffic	Displays the DECnet traffic statistics (including datagrams sent, received, and forwarded).
show disk:0	Displays flash or file system information for a disk located in slot 0:
show dmvpn details	Displays detail DMVPN information for each session, including Next Hop Server (NHS) and NHS status, crypto session information, and socket details.
show environment	Displays temperature, voltage, and blower information on the Cisco 7000 series routers, Cisco 7200 series routers, Cisco 7500 series routers, Cisco 7600 series routers, Cisco AS5300 series access servers, and the Gigabit Switch Router.
show fabric channel counters	Displays the fabric channel counters for a module.
show file system	Lists available file systems.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
show interfaces trunk	Displays the interface-trunk information.
show inventory	Displays the product inventory listing and UDI of all Cisco products installed in the networking device.
show ip interface	Displays the usability status of interfaces configured for IP.
show ip traffic	Displays statistics about IP traffic.
show ip wccp	Displays global statistics related to WCCP.
show logging	Displays the state of syslog and the contents of the standard system logging buffer.
show mac-address table	Displays the MAC address table.
show module	Displays module status and information.
show power	Displays the current power status of system components.
show processes cpu	Displays information about the active processes.
show processes memory	Displays the amount of memory used.

Command	Description
show running-config	Displays the current configuration of your routing device.
show spanning-tree	Displays information about the spanning tree state.
show stacks	Displays the stack usage of processes and interrupt routines.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.
show vlan	Displays VLAN information.

show tech-support ipsec

To display IP Security (IPsec) information to assist in troubleshooting, use the **show tech-support ipsec** command in privileged EXEC mode.

show tech-support ipsec [**peer** *ipv4address* | **vrf** *vrf-name*]

Syntax Description

peer *ipv4address*	(Optional) Displays information for the specified IPv4 peer.
vrf *vrf-name*	(Optional) Displays information for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

The **show tech-support ipsec** simplifies the collection of the IPsec related information if you are troubleshooting a problem. There are three variations of the **show tech-support ipsec** command:

- **show tech-support ipsec**
- **show tech-support ipsec peer** *ipv4address*
- **show tech-support ipsec vrf** *vrf-name*

Output of the show tech-support ipsec Command

If you enter the **show tech-support ipsec** command without any keywords, the command output displays the following **show** commands, in order of output:

- **show version**
- **show running-config**
- **show crypto isakmp sa count**
- **show crypto ipsec sa count**
- **show crypto session summary**
- **show crypto session detail**
- **show crypto isakmp sa detail**
- **show crypto ipsec sa detail**
- **show crypto isakmp peers**
- **show crypto ruleset detail**
- **show processes memory | include Crypto IKMP**
- **show processes cpu | include Crypto IKMP**

- **show crypto eli**
- **show crypto engine accelerator statistic**

Output of the show tech-support ipsec peer Command

If you enter the **show tech-support ipsec** command with the **peer** keyword and the *ipv4address* argument, the output displays the following **show** commands, in order of output for the specified peer:

- **show version**
- **show running-config**
- **show crypto session remote** *ipv4address* **detail**
- **show crypto isakmp sa peer** *ipv4address* **detail**
- **show crypto ipsec sa peer** *ipv4address* **detail**
- **show crypto isakmp peers** *ipv4address*
- **show crypto ruleset detail**
- **show processes memory | include Crypto IKMP**
- **show processes cpu | include Crypto IKMP**
- **show crypto eli**
- **show crypto engine accelerator statistic**

Output of the show tech-support ipsec vrf Command

If you enter the **show tech-support ipsec** command with the **vrf** keyword and the *vrf-name* argument, the output displays the following **show** commands, in order of output for the specified VRF:

- **show version**
- **show running-config**
- **show crypto isakmp sa count vrf** *vrf-name*
- **show crypto ipsec sa count vrf** *vrf-name*
- **show crypto session ivrf** *ivrf-name* **detail**
- **show crypto session fvrf** *fvrf-name* **detail**
- **show crypto isakmp sa vrf** *vrf-name* **detail**
- **show crypto ipsec sa vrf** *vrf-name* **detail**
- **show crypto ruleset detail**
- **show processes memory | include Crypto IKMP**
- **show processes cpu | include Crypto IKMP**
- **show crypto eli**
- **show crypto engine accelerator statistic**

Examples

For a sample display of the output from the **show tech-support ipsec** command, see the documentation for the individual **show** commands listed in the "Usage Guidelines" section.

Related Commands

Command	Description
show tech-support	Displays general information about the router when it reports a problem.

show tunnel endpoints

To display the contents of the tunnel endpoint database that is used for tunnel endpoint address resolution, when running a tunnel in multipoint generic routing encapsulation (mGRE) mode, use the **show tunnel endpoints** command in privileged EXEC mode.

show tunnel endpoints [**tunnel** *tunnel-number*]

Syntax Description

tunnel	(Optional) Specifies the tunnel interface. If a tunnel is specified, only the endpoint database for that tunnel is displayed. If a tunnel is not specified, endpoint databases for all tunnels are displayed.
tunnel-number	(Optional) Tunnel interface number. The range is from 0 to 2147483647.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

The output of **show tunnel endpoints** command displays the tunnel destination and transport address together with any overlay or virtual private network (VPN) address that resolves to it.

Examples

The following example shows that there are two tunnel endpoints in the database that are associated with tunnel 1 (192.0.2.0 and 192.0.2.1). Through these endpoints, VPN destination 192.0.2.3 is reachable by tunneling to endpoint 192.0.2.0 and VPN destination 192.0.2.2 is reachable by tunneling to endpoint 192.0.2.1.

```
Router# show tunnel endpoints

Tunnel0 running in multi-GRE/IP mode

 Endpoint transport 20.20.20.20 Refcount 4 Base 0x55BCC5E8 Create Time 00:01:08
   overlay ::FFFF:20.20.20.20 Refcount 2 Parent 0x55BCC5E8 Create Time 00:01:08
   overlay 20.20.20.20 Refcount 2 Parent 0x55BCC5E8 Create Time 00:01:08
```

Table 192 describes the significant fields shown in the display..

Table 192 show tunnel endpoints Field Descriptions

Field	Description
Transport	Displays the transport address.
Refcount	Number of overlay addresses that are resolving through the destination address.
Base	Displays the base address.
Overlay	Displays the overlay address.
Parent	Reference to the tunnel endpoint.

Related Commands

Command	Description
tunnel mode	Sets the encapsulation mode for the tunnel interface.
tunnel protection	Associates a tunnel interface with an IPSec profile.

show usb controllers

To display USB host controller information, use the **show usb controllers** command in privileged EXEC mode.

show usb controllers [*controller-number*]

Syntax Description

controller-number	(Optional) Displays information only for the specified controller.

Defaults

Information about all controllers on the system are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.

Usage Guidelines

Use the **show usb controllers** command to display content such as controller register specific information, current asynchronous buffer addresses, and period scheduling information. You can also use this command to verify that copy operations are occurring successfully onto a USB flash module.

Examples

The following example is sample output from the **show usb controllers** command:

```
Router# show usb controllers

Name:1362HCD
Controller ID:1
Controller Specific Information:
    Revision:0x11
    Control:0x80
    Command Status:0x0
    Hardware Interrupt Status:0x24
    Hardware Interrupt Enable:0x80000040
    Hardware Interrupt Disable:0x80000040
    Frame Interval:0x27782EDF
    Frame Remaining:0x13C1
    Frame Number:0xDA4C
    LSThreshold:0x628
    RhDescriptorA:0x19000202
    RhDescriptorB:0x0
    RhStatus:0x0
    RhPort1Status:0x100103
    RhPort2Status:0x100303
    Hardware Configuration:0x3029
    DMA Configuration:0x0
    Transfer Counter:0x1
    Interrupt:0x9
```

```
    Interrupt Enable:0x196
    Chip ID:0x3630
    Buffer Status:0x0
    Direct Address Length:0x80A00
    ATL Buffer Size:0x600
    ATL Buffer Port:0x0
    ATL Block Size:0x100
    ATL PTD Skip Map:0xFFFFFFFF
    ATL PTD Last:0x20
    ATL Current Active PTD:0x0
    ATL Threshold Count:0x1
    ATL Threshold Timeout:0xFF

Int Level:1
Transfer Completion Codes:
         Success              :920            CRC              :0
         Bit Stuff            :0              Stall            :0
         No Response          :0              Overrun          :0
         Underrun             :0              Other            :0
         Buffer Overrun       :0              Buffer Underrun :0
Transfer Errors:
         Canceled Transfers   :2              Control Timeout :0
Transfer Failures:
         Interrupt Transfer   :0              Bulk Transfer   :0
         Isochronous Transfer :0              Control Transfer:0
Transfer Successes:
         Interrupt Transfer   :0              Bulk Transfer   :26
         Isochronous Transfer :0              Control Transfer:894

USBD Failures:
         Enumeration Failures :0              No Class Driver Found:0
         Power Budget Exceeded:0

USB MSCD SCSI Class Driver Counters:
         Good Status Failures :3              Command Fail    :0
         Good Status Timed out:0              Device not Found:0
         Device Never Opened  :0              Drive Init Fail :0
         Illegal App Handle   :0              Bad API Command :0
         Invalid Unit Number  :0              Invalid Argument:0
         Application Overflow :0              Device in use   :0
         Control Pipe Stall   :0              Malloc Error    :0
         Device Stalled       :0              Bad Command Code:0
         Device Detached      :0              Unknown Error   :0
         Invalid Logic Unit Num:0

USB Aladdin Token Driver Counters:
         Token Inserted       :1              Token Removed   :0
         Send Insert Msg Fail :0              Response Txns   :434
         Dev Entry Add Fail   :0              Request Txns    :434
         Dev Entry Remove Fail:0              Request Txn Fail:0
         Response Txn Fail    :0              Command Txn Fail:0
         Txn Invalid Dev Handle:0

USB Flash File System Counters:
         Flash Disconnected   :0              Flash Connected :1
         Flash Device Fail    :0              Flash Ok        :1
         Flash startstop Fail :0              Flash FS Fail   :0

USB Secure Token File System Counters:
         Token Inserted       :1              Token Detached  :0
         Token FS success     :1              Token FS Fail   :0
         Token Max Inserted   :0              Create Talker Failures:0
         Token Event          :0              Destroy Talker Failures:0
         Watched Boolean Create Failures:0
```

show usb device

To display USB device information, use the **show usb device** command in privileged EXEC mode.

show usb device [*controller-ID* [*device-address*]]

Syntax Description

controller-ID	(Optional) Displays information only for the devices under the specified controller.
device-address	(Optional) Displays information only for the device with the specified address.

Defaults

Information for all devices attached to the system are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.

Usage Guidelines

Use the **show usb device** command to display information for either a USB flash drive or a USB eToken, as appropriate.

Examples

The following example is sample output from the **show usb device** command:

```
Router# show usb device

Host Controller:1
Address:0x1
Device Configured:YES
Device Supported:YES
Description:DiskOnKey
Manufacturer:M-Sys
Version:2.0
Serial Number:0750D84030316868
Device Handle:0x1000000
USB Version Compliance:2.0
Class Code:0x0
Subclass Code:0x0
Protocol:0x0
Vendor ID:0x8EC
Product ID:0x15
Max. Packet Size of Endpoint Zero:64
Number of Configurations:1
Speed:Full
Selected Configuration:1
Selected Interface:0
```

```
Configuration:
    Number:1
    Number of Interfaces:1
    Description:
    Attributes:None
    Max Power:140 mA

    Interface:
        Number:0
        Description:
        Class Code:8
        Subclass:6
        Protocol:80
        Number of Endpoints:2

        Endpoint:
            Number:1
            Transfer Type:BULK
            Transfer Direction:Device to Host
            Max Packet:64
            Interval:0

        Endpoint:
            Number:2
            Transfer Type:BULK
            Transfer Direction:Host to Device
            Max Packet:64
            Interval:0

Host Controller:1
Address:0x11
Device Configured:YES
Device Supported:YES
Description:eToken Pro 4254
Manufacturer:AKS
Version:1.0
Serial Number:
Device Handle:0x1010000
USB Version Compliance:1.0
Class Code:0xFF
Subclass Code:0x0
Protocol:0x0
Vendor ID:0x529
Product ID:0x514
Max. Packet Size of Endpoint Zero:8
Number of Configurations:1
Speed:Low
Selected Configuration:1
Selected Interface:0

Configuration:
    Number:1
    Number of Interfaces:1
    Description:
    Attributes:None
    Max Power:60 mA

    Interface:
        Number:0
        Description:
        Class Code:255
        Subclass:0
        Protocol:0
        Number of Endpoints:0
```

Table 193 describes the significant fields shown in the display.

Table 193 show usb device Field Descriptions

Field	Description
Device handle	Internal memory handle allocated to the device.
Device Class code	The class code supported by the device. This number is allocated by the USB-IF. If this field is reset to 0, each interface within a configuration specifies its own class information, and the various interfaces operate independently. If this field is set to a value between 1 and FEH, the device supports different class specifications on different interfaces, and the interfaces may not operate independently. This value identifies the class definition used for the aggregate interfaces. If this field is set to FFH, the device class is vendor-specific.
Device Subclass code	The subclass code supported by the device. This number is allocated by the USB-IF.
Device Protocol	The protocol supported by the device. If this field is set to 0, the device does not use class-specific protocols on a device basis. If this field is set to 0xFF, the device uses a vendor-specific protocol on a device basis.
Interface Class code	The class code supported by the interface. If the value is set to 0xFF, the interface class is vendor specific. All other values are allocated by the USB-IF.
Interface Subclass code	The subclass code supported by the interface. All values are allocated by the USB-IF.
Interface Protocol	The protocol code supported by the interface. If this field is set to 0, the device does not use a class-specific protocol on this interface. If this field is set to 0xFF, the device uses a vendor-specific protocol for this interface.
Max Packet	Maximum data packet size, in bytes.

show usb driver

To display information about registered USB class drivers and vendor-specific drivers, use the **show usb driver** command in privileged EXEC mode.

show usb driver [*index*]

Syntax Description

index	(Optional) Displays information only for drivers on the specified index.

Defaults

Information about all drivers is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.

Examples

The following example is sample output for the **show usb driver** command:

```
Router# show usb driver

Index:0
Owner Mask:0x6
Class Code:0x0
Subclass Code:0x0
Protocol:0x0
Interface Class Code:0x8
Interface Subclass Code:0x6
Interface Protocol Code:0x50
Product ID:0x655BD598
Vendor ID:0x64E90000
Attached Devices:
    Controller ID:1, Device Address:1

Index:1
Owner Mask:0x1
Class Code:0x0
Subclass Code:0x0
Protocol:0x0
Interface Class Code:0x0
Interface Subclass Code:0x0
Interface Protocol Code:0x0
Product ID:0x514
Vendor ID:0x529
Attached Devices:
    Controller ID:1, Device Address:17

Index:2
Owner Mask:0x5
Class Code:0x9
```

```
Subclass Code:0x6249BD58
Protocol:0x2
Interface Class Code:0x5DC0
Interface Subclass Code:0x5
Interface Protocol Code:0xFFFFFFFF
Product ID:0x2
Vendor ID:0x1
Attached Devices:
    None

Index:3
Owner Mask:0x10
Class Code:0x0
Subclass Code:0x0
Protocol:0x0
Interface Class Code:0x0
Interface Subclass Code:0x0
Interface Protocol Code:0x0
Product ID:0x0
Vendor ID:0x0
Attached Devices:
    None
```

Table 194 describes the significant field shown in the display.

Table 194 show usb driver Field Descriptions

Field	Description
Owner Mask	Indicates the fields that are used in enumeration comparison. The driver can own different devices on the basis of their product or vendor IDs and device or interface class, subclass, and protocol codes.

show usb port

To sisplay USB root hub port information, use the **show usb port** command in privileged EXEC mode.

show usb port [*port-number*]

Syntax Description

port-number	(Optional) Displays information only for a specified. If the *port-number* is not issued, information for all root ports will be displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

The following sample from the **show usb port** command shows the status of the port 1 on the router:

```
Router# show usb port

Port Number:0
Status:Enabled
Connection State:Connected
Speed:Full
Power State:ON

Port Number:1
Status:Enabled
Connection State:Connected
Speed:Low
Power State:ON
```

show usb tree

To display information about the port state and all attached devices, use the **show usb tree** command in privileged EXEC mode.

show usb tree

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

The following example is sample output from the **show usb tree** command. This output shows that both a USB flash module and a USB eToken are currently enabled.

```
Router# show usb tree

[Host Id:1, Host Type:1362HCD, Number of RH-Port:2]
<Root Port0:Power=ON      Current State=Enabled>
  Port0:(DiskOnKey) Addr:0x1 VID:0x08EC PID:0x0015 Configured (0x1000000)
<Root Port1:Power=ON      Current State=Enabled>
  Port1:(eToken Pro 4254) Addr:0x11 VID:0x0529 PID:0x0514 Configured (0x1010000)
```

show usbtoken

To display information about the USB eToken (such as the eToken ID), use the **show usbtoken** command in privileged EXEC mode.

show usbtoken[**0-9**]**:**[**all** | *filesystem*]

Syntax Description

0-9	(Optional) One of the ten available flash drives you can choose from; valid values: 0-9. If you do not specify a number, 0 is used by default
all	(Optional) All configuration files stored on the eToken.
filesystem	(Optional) Name of a configuration file.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.

Usage Guidelines

Use the **show usbtoken** command to verify whether a USB eToken is inserted in the router.

Examples

The following example is sample output from the **show usbtoken** command:

```
Router# show usbtoken0

Token ID           :43353334
Token device name  : token0
Vendor name        : Vendor34
Product Name       :Etoken Pro
Serial number      : 22273a334353
Firmware version   :   4.1.3.2
Total memory size  : 32 KB
Free memory size   : 16 KB
FIPS version       :  Yes/No
Token state        :  "Active" | "User locked" | "Admin locked" | "System Error" |
"Uknown"
ATR (Answer To Reset) :"3B F2 98 0  FF C1 10 31 FE 55 C8 3"
```

Table 195 describes the significant fields shown in the display.

Table 195 show usbtoken Field Descriptions

Field	Description
Token ID	Token identifier.

Table 195 show usbtoken Field Descriptions (continued)

Field	Description
Token device name	A unique name derived by the token driver.
ATR (Answer to Reset)	Information replied by Smart cards when a reset command is issued.

show user-group

To display information about user groups, use the **show user-group** command in privileged EXEC mode.

show user-group [*group-name* | **count**]

Syntax Description

group-name	(Optional) Name of the user-group.
count	(Optional) Displays the total number of user groups, the names of the user groups, and the number of members in each.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following is sample output from the **show user-group** command when the auth_proxy_ug user group is specified.

```
Router# show user-group auth_proxy_ug
!
Usergroup: auth_proxy_ug
------------------------------------------------------------------
User Name          Type    Interface  Learn      Age (min)
------------------------------------------------------------------
192.168.101.131    IPv4    Vlan333    Dynamic    0
!
```

The following is sample output from the **show user-group** command when the **count** keyword is used.

```
Router# show user-group count
!
Total Usergroup: 2
--------------------------
User Group     Members
--------------------------
auth_proxy_ug  1
eng_group_ug   1
!
```

Table 196 describes the significant fields shown in the displays.

Table 196 show user-group Field Descriptions

Field	Description
User Name	IP address of the user-group.
Learn	Describes how the mapping of source IP addresses to user groups is learned.

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
user-group	Defines the user-group associated with the identity policy.

show users

To display information about the active lines on the router, use the **show users** command in user EXEC or privileged EXEC mode.

show users [[**all**] [**wide**] | **slot** {*slot-number* | **all**} | **summary**] [**lawful-intercept**]

Syntax Description

all	(Optional) Specifies that all lines be displayed, regardless of whether anyone is using them.
wide	(Optional) Specifies that the wide format be used.
slot	(Optional) Displays information about remote logins to other processes in the chassis.
slot-number	(Optional) The slot number.
summary	(Optional) Displays a summary of user sessions.
lawful-intercept	(Optional) Displays lawful-intercept users.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.3(2)T	The **summary** keyword was introduced.
12.3(7)T	The **lawful-intercept** keyword was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXI	This command was modified in a release earlier than Cisco IOS Release 12.2(33)SXI. The **slot** keyword and *slot-number* argument were added.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Sevices Routers.

Usage Guidelines

This command displays the line number, connection name, idle time, hosts (including virtual access interfaces), and terminal location. An asterisk (*) indicates the current terminal session.

If the **lawful-intercept** keyword is issued, the names of all users who have access to a configured lawful intercept view will be displayed. To access the **show users lawful-intercept** command, you must be an authorized lawful-intercept-view user.

When an idle timeout is configured on a full virtual access interface and a subvirtual access interface, the **show users** command displays the idle time for both the interfaces. However, if the idle timeout is not configured on both the interfaces, then the **show users** command will display the idle time for the full virtual access interface only.

Examples

The following is sample output from the **show users** command:

```
Router# show users

     Line          User           Host(s)       Idle Location
     0 con 0                      idle
*    2 vty 0       user1          idle           0   SERVICE1.CISCO.COM
```

The following is sample output identifying an active virtual access interface:

```
Router# show users

Line         User      Host(s)                Idle    Location
*  0 con 0             idle                   01:58
  10 vty 0             Virtual-Access2         0      1212321
```

The following is sample output from the **show users all** command:

```
Router# show users all

       Line      User         Host(s)     Idle  Location
*   0 vty 0   user1        idle         0    SERVICE1.CISCO.COM
    1 vty 1
       2 con 0
       3 aux 0
       4 vty 2
```

Table 197 describes the significant fields shown in the displays.

Table 197 show users Field Descriptions

Field	Description
Line	Contains three subfields: • The first subfield (0 in the sample output) is the absolute line number. • The second subfield (vty in the sample output) indicates the type of line. Possible values follow: aux—auxiliary port con—console tty—asynchronous terminal port vty—virtual terminal • The third subfield (0 in the * sample output) indicates the relative line number within the type.
User	User using the line. If no user is listed in this field, no one is using the line.
Host(s)	Host to which the user is connected (outgoing connection). A value of idle means that there is no outgoing connection to a host.
Idle	Interval (in minutes) since the user has entered something.
Location	Either the hard-wired location for the line or, if there is an incoming connection, the host from which the incoming connection came.

The following sample output from the **show users lawful intercept** command shows three LI-View users on the system—li_admin, li-user1, and li-user2:

```
Router# show users lawful-intercept

li_admin
li-user1
li-user2
Router#
```

Related Commands

Command	Description
line	Identifies a specific line for configuration and starts the line configuration command collection mode.
li-view	Initializes a lawful intercept view.
show line	Displays the parameters of a terminal line.
username	Establishes a username-based authentication system.

show vasi pair

To display the status of a VRF-Aware Service Infrastructure (VASI) pair, use the **show vasi pair** command in privileged EXEC mode.

show vasi pair status [*number*]

Syntax Description

status	Displays the VASI pair status.
number	(Optional) VASI pair number. The range is from 1 to 256.

Command Default

If no interface is specified, all VASI interfaces are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Examples

The following is sample output from the **show vasi pair** command:

```
Router# show vasi pair status 100

Pair name     Left state            Right state           Pair state
------------------------------------------------------------------------------
VASIPair100   down                  not configured        need vasiright100
```

Table 198 describes the significant fields shown in the display.

Table 198 show vasi pair status Field Descriptions

Field	Description
Pair name	Name of the VASI interface pair.
Left state	State of the vasileft interface. The values are as follows: • admin down—interface is administratively down. • down—interface is down. • not configure—interface is not configured. • up—interface is operational and up.

Table 198 show vasi pair status Field Descriptions (continued)

Field	Description
Right state	State of the vasiright interface. The values are as follows: • admin down—interface is administratively down. • down—interface is down. • not configure—interface is not configured. • up—interface is operational and up.
Pair state	Vasi pair status. Possible values are as follows: • need vasileft—vasileft interface is not configured. • need vasiright—vasiright interface is not configured. • up— both interfaces are up and operational. • vasileft down—vasileft interface state is down • vasiright down—vasiright interface state is down

Related Commands

debug adjacency (vasi)	Displays debugging information for VASI adjacency.
debug interface (vasi)	Displays debugging information for VASI interface descriptor block.
debug vasi	Displays VASI debugging information.
interface (vasi)	Configures a VASI virtual interface.

show vlan group

To display the VLANs mapped to VLAN groups, use the **show vlan group** command in privileged EXEC mode.

show vlan group [**group-name** *group-name*]

Syntax Description

group-name *group-name*	(Optional) Displays the VLANs mapped to the specified VLAN group.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI1	This command was introduced.

Usage Guidelines

The **show vlan group** command displays the existing VLAN groups and lists the VLANs and VLAN ranges that are members of each VLAN group. If the **group-name** keyword is entered, only the members of the VLAN group specified by the *group-name* argument are displayed.

Examples

This example shows how to display the members of a specified VLAN group:

```
Router# show vlan group group-name ganymede

Group Name Vlans Mapped
---------------- --------------------
ganymede         7-9
```

Related Commands

Command	Description
vlan group	Creates or modifies a VLAN group.

show vtemplate

To display information about all configured virtual templates, use the **show vtemplate** command in privileged EXEC mode.

show vtemplate

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)DC	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(14)T	The show display was modified to display the interface type of the virtual template and to provide counters on a per-interface-type basis for IPsec virtual tunnel interfaces.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following is sample output from the **show vtemplate** command:

```
Router# show vtemplate

Virtual access subinterface creation is globally enabled

         Active     Active    Subint  Pre-clone Pre-clone Interface
       Interface Subinterface Capable Available   Limit     Type
       --------- ------------ ------- --------- --------- ---------
Vt1            0            0   Yes          --        --   Serial
Vt2            0            0   Yes          --        --   Serial
Vt4            0            0   Yes          --        --   Serial
Vt21           0            0    No          --        --   Tunnel
Vt22           0            0   Yes          --        --   Ether
Vt23           0            0   Yes          --        --   Serial
Vt24           0            0   Yes          --        --   Serial

Usage Summary
                              Interface   Subinterface
                              ---------   ------------
Current Serial  in use                1              0
Current Serial  free                  0              3
Current Ether   in use                0              0
Current Ether   free                  0              0
Current Tunnel  in use                0              0
Current Tunnel  free                  0              0
Total                                 1              3

Cumulative created                    8              4
Cumulative freed                      0              4
```

```
Base virtual access interfaces: 1
Total create or clone requests: 0
Current request queue size: 0
Current free pending: 0

Maximum request duration: 0 msec
Average request duration: 0 msec
Last request duration: 0 msec

Maximum processing duration: 0 msec
Average processing duration: 0 msec
Last processing duration: 0 msec
Last processing duration:0 msec
```

Table 199 describes the significant fields shown in the example.

Table 199 show vtemplate Field Descriptions

Field	Description
Virtual access subinterface creation is globally...	The configured setting of the **virtual-template** command. Virtual access subinterface creation may be enabled or disabled.
Active Interface	The number of virtual access interfaces that are cloned from the specified virtual template.
Active Subinterface	The number of virtual access subinterfaces that are cloned from the specified virtual template.
Subint Capable	Specifies if the configuration of the virtual template is supported on the virtual access subinterface.
Pre-clone Available	The number of precloned virtual access interfaces currently available for use for the particular virtual template.
Pre-clone Limit	The number of precloned virtual access interfaces available for that particular virtual template.
Current in use	The number of virtual access interfaces and subinterfaces that are currently in use.
Current free	The number of virtual access interfaces and subinterfaces that are no longer in use.
Total	The total number of virtual access interfaces and subinterfaces that exist.
Cumulative created	The number of requests for a virtual access interface or subinterface that have been satisfied.
Cumulative freed	The number of times that the application using the virtual access interface or subinterface has been freed.
Base virtual-access interfaces	This field specifies the number of base virtual access interfaces. The base virtual access interface is used to create virtual access subinterfaces. There is one base virtual access interface per application that supports subinterfaces. A base virtual access interface can be identified from the output of the **show interfaces virtual-access** command.
Total create or clone requests	The number of requests that have been made through the asynchronous request API of the virtual template manager.

Table 199 show vtemplate Field Descriptions (continued)

Field	Description
Current request queue size	The number of items in the virtual template manager work queue.
Current free pending	The number of virtual access interfaces whose final freeing is pending. These virtual access interfaces cannot currently be freed because they are still in use.
Maximum request duration	The maximum time that it took from the time that the asynchronous request was made until the application was notified that the request was done.
Average request duration	The average time that it took from the time that the asynchronous request was made until the application was notified that the request was done.
Last request duration	The time that it took from the time that the asynchronous request was made until the application was notified that the request was done for the most recent request.
Maximum processing duration	The maximum time that the virtual template manager spent satisfying the request.
Average processing duration	The average time that the virtual template manager spent satisfying the request.
Last processing duration	The time that the virtual template manager spent satisfying the request for the most recent request.

Related Commands

Command	Description
clear counters	Clears interface counters.
show interfaces virtual-access	Displays status, traffic data, and configuration information about a specified virtual access interface.
virtual-template	Specifies which virtual template will be used to clone virtual access interfaces.

show webvpn context

To display the operational status and configuration parameters for Secure Socket Layer (SSL) virtual private network (VPN) context configurations, use the **show webvpn context** command in privileged EXEC mode.

show webvpn context [*name* | **brief**]

Syntax Description

name	(Optional) Name of the context for which output will be filtered to display detailed information.
brief	(Optional) Filters the output to display a summary of SSL VPN context configuration.

Command Default

If no arguments or keywords are specified, the output displays general information about the operational status of all SSL VPN contexts.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.0(1)M	This command was modified. The **brief** keyword was added.

Usage Guidelines

Entering a context name displays more detailed information, such as the operational status and specific configuration information for the named context.

Examples

The following output is an example of brief information that can be displayed for system security officer (SSO) servers configured for the SSL VPN context:

```
Router# show webvpn context brief

Codes: AS - Admin Status, OS - Operation Status
       VHost - Virtual Host

Context Name        Gateway  Domain/VHost      VRF      AS    OS
------------        -------  ------------      -------  ----  --------
Default_context     n/a      n/a               n/a      down  down
con-1               gw-1     one               -        up    up
con-2               -        -                 -        down  down
```

Table 200 describes the significant fields shown in the display.

Table 200 show webvpn context brief Field Descriptions

Field	Description
Context Name	Displays the name of the context.
Gateway	Displays the name of the associated gateway. n/a is displayed if no gateway is associated.
Domain/VHost	Displays the SSL VPN domain or virtual hostname.
VRF	Displays the VPN routing and forwarding (VRF) instance, if configured, that is associated with the context configuration.
AS	Displays the administrative status of the SSL VPN context. The status is displayed as “up” or “down.”
OS	Displays the operational status of the SSL VPN context. The status is displayed as “up” or “down.”

The following is sample output from the **show webvpn context** command entered with the name of a specific SSL VPN context:

```
Router# show webvpn context 1234567891234567891second

Admin Status: down
Operation Status: down
Error and Event Logging: Disabled
CSD Status: Disabled
Certificate authentication type: All attributes (like CRL) are verified
AAA Authentication List not configured
AAA Authorization List not configured
AAA Accounting List not configured
AAA Authentication Domain not configured
Authentication mode: AAA authentication
Default Group Policy not configured
Not associated with any WebVPN Gateway
Domain Name and Virtual Host not configured
Maximum Users Allowed: 1000 (default)
NAT Address not configured
VRF Name not configured
Virtual Template not configured
```

Table 201 describes the significant fields shown in the display.

Table 201 show webvpn context (Specific WebVPN Context) Field Descriptions

Field	Description
Admin Status	Administrative status of the context. The status is displayed as “up” or “down.” The **inservice** command is used to configure this configuration parameter.
Operation Status	Displays the operational status of the SSL VPN. The status is displayed as “up” or “down.” The context and the associated gateway must both be in an enabled state for the operational status to be “up.”
CSD Status	Displays the status of Cisco Secure Desktop (CSD). The status is displayed as “Enabled” or “Disabled.”
Certificate authentication type	Displays the certification authority (CA) type.

Table 201 show webvpn context (Specific WebVPN Context) Field Descriptions (continued)

Field	Description
AAA Authentication List...	Displays the authentication list if configured.
AAA Authentication Domain...	Displays the authentication, authorization, and accounting (AAA) domain if configured.
Default Group Policy	Name of the group policy configured under the named context.
Domain Name	Domain name or virtual hostname configured under the named context.
Maximum Users Allowed	Displays the maximum number of user sessions that can be configured.
NAT Address...	Displays the Network Address Translation (NAT) address if configured.
VRF	Displays the VRF, if configured, that is associated with the context configuration.

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

show webvpn gateway

To display the status of a SSL VPN gateway, use the **show webvpn gateway** command in privileged EXEC mode.

show webvpn gateway [*name*]

Syntax Description

name	(Optional) Filters the output to display more detailed information about the named gateway.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Entering this command without specifying a gateway name, displays general the operational status of all SSL VPN gateways. Entering a gateway name displays the IP address and CA trustpoint.

Examples

The following is sample output from the **show webvpn gateway** command:

```
Router# show webvpn gateway

Gateway Name                    Admin  Operation
------------                    -----  ---------
GW_1                            up     up
GW_2                            down   down
```

Table 202 describes the significant fields shown in the display.

Table 202 show webvpn gateway Field Descriptions

Field	Description
Gateway Name	Name of the gateway.
Admin	The administrative status of the gateway, displayed as “up” or “down.” Administrative status is configured with the **inservice** command.
Operation	The operational status of the gateway, displayed as “up” or “down.” The gateway must be “inservice” and configured with a valid IP address to be in an “up” state.

The following is sample output from the **show webvpn gateway** command, entered with a specific SSL VPN gateway name:

```
Router# show webvpn gateway GW_1

Admin Status: up
Operation Status: up
IP: 10.1.1.1, port: 443
SSL Trustpoint: TP-self-signed-26793562
```

Table 203 describes the significant fields shown in the display.

Table 203 show webvpn gateway name Field Descriptions

Field	Description
Admin Status	The administrative status of the gateway, displayed as “up” or “down.” Administrative status is configured with the **inservice** command.
Operation Status	The operational status of the gateway, displayed as “up” or “down.” The gateway must be “inservice” and configured with a valid IP address to be in an “up” state.
IP: ... port: ...	The configured IP address and port number of the WebVPN gateway. The default port number 443.
SSL Trustpoint:	Configures the CA certificate trust point.

Related Commands

Command	Description
webvpn gateway	Enters webvpn gateway configuration mode to configure a SSL VPN gateway.

show webvpn install

To display the installation status of SVC or CSD client software packages, use the **show webvpn install** command in EXEC mode.

show webvpn install {**file** *name* | **package** {**csd** | **svc**} | **status** {**csd** | **svc**}}

Syntax Description

file *name*	Displays file attribute information about the named software package file.
package {**csd**	**svc**}	Displays information about either the CSD or SVC software installation package.
status {**csd**	**svc**}	Displays file attribute information about the CSD or SVC software package.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command is used to display information about Cisco Secure Desktop (CSD) and SSL VPN Client (SVC) software pages that are locally cached for distribution to remote SSL VPN clients. This information includes software versions and build dates.

Examples

The following is sample output from the **show webvpn install** command, entered with the **file** keyword:

```
Router# show webvpn install file \webvpn\stc\version.txt

SSLVPN File \webvpn\stc\version.txt installed:
CISCO STC win2k+ 1.0.0
1,1,0,116
Fri 06/03/2005 03:02:46.43
```

Table 204 describes the significant fields shown in the display.

Table 204 show webvpn install file Field Descriptions

Field	Description
SSLVPN File	The local path to the specified installation package file. File attributes, such as the name, build number, and installation date are deployed following this line.

The following is sample output from the **show webvpn install** command, entered with the **package svc** keywords:

```
Router# show webvpn install package svc

SSLVPN Package SSL-VPN-Client installed:
File: \webvpn\stc\1\binaries\detectvm.class, size: 555
File: \webvpn\stc\1\binaries\java.htm, size: 309
File: \webvpn\stc\1\binaries\main.js, size: 8049
File: \webvpn\stc\1\binaries\ocx.htm, size: 244
File: \webvpn\stc\1\binaries\setup.cab, size: 176132
File: \webvpn\stc\1\binaries\stc.exe, size: 94696
File: \webvpn\stc\1\binaries\stcjava.cab, size: 7166
File: \webvpn\stc\1\binaries\stcjava.jar, size: 4846
File: \webvpn\stc\1\binaries\stcweb.cab, size: 13678
File: \webvpn\stc\1\binaries\update.txt, size: 11
File: \webvpn\stc\1\empty.html, size: 153
File: \webvpn\stc\1\images\alert.gif, size: 2042
File: \webvpn\stc\1\images\buttons.gif, size: 1842
File: \webvpn\stc\1\images\loading.gif, size: 313
File: \webvpn\stc\1\images\title.gif, size: 2739
File: \webvpn\stc\1\index.html, size: 4725
File: \webvpn\stc\2\index.html, size: 325
File: \webvpn\stc\version.txt, size: 63
Total files: 18
```

Table 205 describes the significant fields shown in the display.

Table 205 show webvpn install package Field Descriptions

Field	Description
SSLVPN Package SSL-VPN-Client installed:	Displays the installation status of the CSD or SVC software package as “installed” or “NONE.”
File: ... size: ...	The path, name, and size of each installation file.
Total files:	Total number in the package.

The following is sample output from the **show webvpn install** command, entered with the **status svc** keywords:

```
Router# show webvpn install status svc

SSLVPN Package SSL-VPN-Client version installed:
CISCO STC win2k+ 1.0.0
1,0,2,127
Fri 07/22/2005 12:14:45.43
```

Table 206 describes the significant fields shown in the display.

Table 206 show webvpn install stats Field Descriptions

Field	Description
SSLVPN Package	The SVC or CSD package file status is displayed as “installed” or “NONE.” File attributes, such as the name, build number, and installation date are displayed following this line.

Related Commands

Command	Description
webvpn install	Installs a CSD or SVC package file to a WebVPN gateway for distribution to remote users.

show webvpn license

To display the available count and the current usage, use the **show webvpn license** command in privileged EXEC mode.

show webvpn license

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Use the **show webvpn license** command to display the available count and the current usage. To display the current license type and time period left in the case of a nonpermanent licence, use the **show license** command.

Examples

The following is sample output from the **show webvpn license** command:

```
Router# show webvpn license

Available license count : 200
Reserved license count  : 200
In-use count : 3
```

The above output is self-explanatory.

Related Commands

Command	Description
debug webvpn license	Displays debug messages related to license operations, events, and errors.

show webvpn nbns

To display information in the NetBIOS Name Service (NBNS) cache, use the **show webvpn nbns** command in privileged EXEC mode.

show webvpn nbns {**context** {**all** | *name*}}

Syntax Description

context *name*	Filters the output to display NBNS information for the named context.
context all	Displays NBNS information for all contexts.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command is used to display information about NBNS cache entries. The NetBIOS name, IP address of the Windows Internet Name Service (WINS) server, and associated time stamps.

Examples

The following is sample output from the **show webvpn nbns** command, entered with the **context** and **all** keywords:

```
Router# show webvpn nbns context all

NetBIOS name        IP Address       Timestamp

0 total entries
NetBIOS name        IP Address       Timestamp

0 total entries
NetBIOS name        IP Address       Timestamp

0 total entries
```

Table 207 describes the significant fields shown in the display.

Table 207 show webvpn nbns context all Field Descriptions

Field	Description
NetBIOS name	NetBIOS name.
IP Address	The IP address of the WINs server.

Table 207 show webvpn nbns context all Field Descriptions (continued)

Field	Description
Timestamp	Time stamp for the last entry.
... total entries	Total number of NetBIOS cache entries.

Related Commands

Command	Description
nbns-list	Enters webvpn NBNS list configuration mode to configure a NBNS server list for CIFS name resolution.
webvpn install	Installs a CSD or Cisco AnyConnect VPN Client package file to a SSL VPN gateway for distribution to end users.

show webvpn policy

To display the context configuration associated with a policy group, use the **show webvpn policy** command in user EXEC or privileged EXEC mode.

show webvpn policy group *name* **context** {**all** | *name*} [**detail**]

Syntax Description

group *name*	Displays information for the named policy group.
context all	Displays information for all context configurations with which the policy group is associated.
context *name*	Displays information for the named context configuration.
detail	(Optional) Displays detailed information about the user session.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(11)T	This command was modified. An output example was added for Single SignOn (SSO) server information.
15.1(1)T	This command was modified. The **detail** keyword was added. The output was modified to display the webvpn home page configuration.

Usage Guidelines

This command is used to display configuration settings that apply only to the policy group. This command can also be used to display all contexts for which the policy group is configured.

Examples

The following is sample output from the **show webvpn policy** command:

```
Router# show webvpn policy group group1 context all

WEBVPN: group policy = group1 ; context = context1
      url list name = "web-url"
      cifs url list name = "cifs-url"
      idle timeout = 2100 sec
      session timeout = Disabled
      port forward name = "pflist"
      functions =
                file-access
                file-browse
                file-entry
                svc-enabled

      citrix disabled
      address pool name = "70pool"
      svc home page = "http://wiki-eng.cisco.com/engwiki/SSLVPNTech"
      webvpn home page = "http://192.0.2.0", redirection time = 10
      dpd client timeout = 300 sec
```

```
      dpd gateway timeout = 300 sec
      keepalive interval = 30 sec
      SSLVPN Full Tunnel mtu size = 1406 bytes
      keep sslvpn client installed = enabled
      rekey interval = 3600 sec
      rekey method =
      lease duration = 43200 sec
      msie-proxy = auto
      ie proxy server = "test.com:80"
      split include = 209.165.200.225 255.255.255.224
      split include = 209.165.200.226 255.255.255.224
```

See Table 208 for the field description.

The following sample output displays information about an SSO server configured for a policy group of the SSL VPN context:

```
Router# show webvpn policy group ONE context all

WV: group policy = sso ; context = test_sso
  idle timeout = 2100 sec
  session timeout = 43200 sec
  sso server name = "server2
  citrix disabled
  dpd client timeout = 300 sec
  dpd gateway timeout = 300 sec
  keep sslvpn client installed = disabled
  rekey interval = 3600 sec
  rekey method =
  lease duration = 43200 sec
```

Table 208 describes the significant fields shown in the displays.

Table 208 show webvpn policy Field Descriptions

Field	Description
group policy	Name of the policy group.
context	Name of the Secure Socket Layer (SSL) Virtual Private Network (VPN) context.
url list name	Name of the URL list.
cifs url list name	Name of the Common Internet File System (CIFS) URL list.
idle timeout	Length of time that a remote-user session can remain idle.
session timeout	Length of time that a remote-user session can remain active.
port forward name	Name of the port-forwarding list configured with the **port-forward** command.
citrix	Support for Citrix applications, shown as “disabled” or “enabled.”
address pool name	Name of the address pool configured.
svc home page	URL of the SSL VPN Client (SVC) configured.
webvpn home page	URL of the WebVPN configured using the **webvpn-homepage** command.
dpd client timeout	Length of time that a session will be maintained with a nonresponsive end user (remote client).

Table 208 show webvpn policy Field Descriptions (continued)

Field	Description
dpd gateway timeout	Length of the time that a session will be maintained with a nonresponsive SSL VPN gateway.
keepalive interval	Keepalive interval, in seconds.
SSLVPN Full Tunnel mtu size	MTU, in bytes.
keep sslvpn client installed	Cisco AnyConnect VPN Client software installation policy on the end user (remote PC). “enabled” indicates that Cisco AnyConnect VPN Client software remains installed after the SSL VPN session is terminated. “disabled” indicates that Cisco AnyConnect VPN Client software is pushed to the end user each time a connection is established.
rekey interval	Length of time between tunnel key refresh cycles.
rekey method	Tunnel key authentication method.
lease duration	Tunnel key lifetime.
sso server name	Name of the SSO server.

Related Commands

Command	Description
policy group	Enters SSL VPN group policy configuration mode to configure a group policy.

show webvpn session

To display Secure Sockets Layer Virtual Private Network (SSL VPN) user session information, use the **show webvpn session** command in user EXEC or privileged EXEC mode.

show webvpn session [**user** *user-name*] **context** {*context-name* | **all**} [**detail**]

Syntax Description

user	(Optional) Displays detailed information about the named user session.
user-name	(Optional) Name of the user.
context	Displays a list of active users for only the named context.
context-name	Name of the context.
all	Displays a list of active users sessions for all locally configured contexts.
detail	(Optional) Displays detailed information about the user session.

Command Default

Session information is not displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.1(1)T	This command was modified. The **detail** keyword was added.

Usage Guidelines

This command is used to list active SSL VPN connections or to display context configuration policies that apply to the specified end user.

The **show webvpn session** command provides detailed information about the user session. These details include the username, assigned IP addess, group policy, login time, hash algorithms used for the session, number of clientless tunnels, and the number of full tunnels enabled for the user.

This command is applicable only for user session statistics and tunnel statistics.

Examples

The following is sample output from the **show webvpn session** command. The output is filtered to display user session information for only the specified context.

```
Router# show webvpn session context context1

WebVPN context name: context1
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
user1              192.0.2.1                  2         04:47:16  00:01:26
user2              192.0.2.2                  2         04:48:36  00:01:56
```

Table 209 describes the significant fields shown in the display.

Table 209 show webvpn session Field Descriptions

Field	Description
WebVPN context name	Name of the context.
Client_Login_Name	Login name for the end user (remote PC or device).
Client_IP_Address	IP address of the remote user.
No_of_Connections	Number of times the remote user has connected.
Created	Time, in hh:mm:ss, when the remote connection was established.
Last_Used	Time, in hh:mm:ss, that the user connection last generated network activity.

The following is sample output from the **show webvpn session** command. The output is filtered to display session information for a specific user.

```
Router# show webvpn session user user1 context all

Session Type      : Full Tunnel
Client User-Agent : Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.5)

Username          : test                 Num Connection : 1
Public IP         : 192.0.2.0            VRF Name       : None
Context           : context1             Policy Group   : default
Last-Used         : 00:00:42             Created        : *09:50:38.191 UTC Thu Jan 21
2010
Session Timeout   : Disabled             Idle Timeout   : 2100
DPD GW Timeout    : 300                  DPD CL Timeout : 300
Address Pool      : varun                MTU Size       : 1206
Rekey Time        : 3600                 Rekey Method   :
Lease Duration    : 43200
Tunnel IP         : 209.165.200.225      Netmask        : 255.255.255.224
Rx IP Packets     : 0                    Tx IP Packets  : 1
CSTP Started      : 00:01:42             Last-Received  : 00:01:42
CSTP DPD-Req sent : 0                    Virtual Access : 1
Msie-ProxyServer  : None                 Msie-PxyPolicy : Disabled
Msie-Exception    :
Split Include     : 209.165.200.224 255.255.255.224
Client Ports      : 2538
DTLS Port         : 2547
```

Table 210 describes the significant fields shown in the display.

Table 210 show webvpn session user context all Field Descriptions

Field	Description
Session Type	Mode used to access SSL VPN.
Client User-Agent	The client user-agent header.
Username	Name of the end user.
Num Connection	Number of times the remote user has connected.
Public IP	Public IP address.
VRF Name	Name of the virtual routing and forwarding (VRF) interface.

Table 210 show webvpn session user context all Field Descriptions (continued)

Field	Description
Context	Name of the context to which user policies apply.
Policy Group	Name of the policy group to which the user belongs.
Last-Used	Time, in hh:mm:ss, that the user connection last generated network activity.
Created	Time, in hh:mm:ss, when the remote connection was established.
Session Timeout	Length of time that a remote-user session can remain active.
Idle Timeout	Length of time that a remote-user session can remain idle.
DPD GW Timeout	Length of time that a Dead Peer Detection (DPD) gateway can remain idle.
DPD CL Timeout	Length of time that a DPD client can remain idle.
Address Pool	Name of the address pool configured.
MTU Size	Size of the maximum transmission unit (MTU).
Rekey Time	Time at which the tunnel key is refreshed.
Rekey Method	Tunnel key authentication method.
Lease Duration	Tunnel key lifetime.
Tunnel IP	IP address of the SSL VPN tunnel.
Netmask	Network mask used.
Rx IP Packets	Number of IP packets sent.
Tx IP Packets	Number of IP packets received.
CSTP Started	Time at which the Cisco SSL Tunnel Protocol (CSTP) frames were sent to the client.
Last-Received	Time when the CSTP frame was received.
CSTP DPD-Req sent	Time at which the CSTP request was sent to the client.
Virtual Access	Total number of virtual access interfaces created.
Msie-ProxyServer	Number of Microsoft Internet Explorer (MSIE) proxy servers configured for policy group end users.
Msie-PxyPolicy	Status of the MSIE policy: Enabled or Disabled.
Msie-Exception	MS Proxy exceptions.
Split Include	IP address from which the traffic is resolved through the Cisco AnyConnect VPN Client tunnel.
Client Ports	Local TCP port used on the client host.
DTLS Port	Datagram Transport Layer Security (DTLS) port.

The following is sample output from the **show webvpn session user context all detail** command:

```
Router# show webvpn session user user1 context all detail

Session Type      : Full Tunnel
Client User-Agent : Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:10.0.0.1)
```

```
Username          : user1                Num Connection : 1
Public IP         : 209.165.200.225      VRF Name       : None
Context           : context1             Policy Group   : default
Last-Used         : 00:00:02             Created        : *09:50:38.191 UTC Thu Jan 21
2010
Session Timeout   : Disabled             Idle Timeout   : 2100
DPD GW Timeout    : 300                  DPD CL Timeout : 300
Address Pool      : varun                MTU Size       : 1206
Rekey Time        : 3600                 Rekey Method   :
Lease Duration    : 43200
Tunnel IP         : 209.165.200.249      Netmask        : 255.255.255.224
Rx IP Packets     : 0                    Tx IP Packets  : 2
CSTP Started      : 00:02:03             Last-Received  : 00:02:03
CSTP DPD-Req sent : 0                    Virtual Access : 1
Msie-ProxyServer  : None                 Msie-PxyPolicy : Disabled
Msie-Exception    :
Split Include     : 209.165.200.250 255.255.255.224
Client Ports      : 2538
DTLS Port         : 2547

Detail Session Statistics for User:: user1
-----------------------------------

CSTP Statistics::
Rx CSTP Frames    : 4                    Tx CSTP Frames   : 0
Rx CSTP Bytes     : 32                   Tx CSTP Bytes    : 0
Rx CSTP Data Fr   : 0                    Tx CSTP Data Fr  : 0
Rx CSTP CNTL Fr   : 4                    Tx CSTP CNTL Fr  : 0
Rx CSTP DPD Req   : 0                    Tx CSTP DPD Req  : 0
Rx CSTP DPD Res   : 0                    Tx CSTP DPD Res  : 0
Rx Addr Renew Req : 0                    Tx Address Renew : 0
Rx CDTP Frames    : 2                    Tx CDTP Frames   : 0
Rx CDTP Bytes     : 122                  Tx CDTP Bytes    : 0
Rx CDTP Data Fr   : 2                    Tx CDTP Data Fr  : 0
Rx CDTP CNTL Fr   : 0                    Tx CDTP CNTL Fr  : 0
Rx CDTP DPD Req   : 0                    Tx CSTP DPD Req  : 0
Rx CDTP DPD Res   : 0                    Tx CDTP DPD Res  : 0
Rx IP Packets     : 0                    Tx IP Packets    : 2
Rx IP Bytes       : 0                    Tx IP Bytes      : 10

CEF Statistics::
Rx CSTP Data Fr   : 0                    Tx CSTP Data Fr  : 0
Rx CSTP Bytes     : 0                    Tx CSTP Bytes    : 0
```

Table 211 describes the significant fields shown in the display.

Table 211 show webvpn session user context all detail Field Descriptions

Field	Description
Rx CSTP Frames	Number of CSTP frames received from the client.
Rx CSTP Bytes	Number of CSTP bytes (data plus control frames) received from the client.
Rx CSTP Data Fr	Number of CSTP data frames received from the client.
Rx CSTP CNTL Fr	Number of CSTP control frames received from the client.
Rx CSTP DPD Req	Number of DPD requests received at the gateway.
Rx CSTP DPD Res	Number of times the gateway processed a CSTP DPD request frame.
Rx Addr Renew Req	Number of address renew requests received at the gateway.

Table 211 show webvpn session user context all detail Field Descriptions (continued)

Field	Description
Rx CDTP Frames	Number of Cisco Dynamic Trunking Protocol (CDTP) frames received from the client.
Rx CDTP Bytes	Number of CDTP bytes received from the client.
Rx CDTP Data Fr	Number of CDTP data frames received from the client.
Rx CDTP CNTL Fr	Number of CDTP control frames received from the client.
Rx CDTP DPD Req	Number of CDTP DPD requests received at the gateway.
Rx CDTP DPD Res	Number of times the gateway processed a CDTP DPD request frame.
Rx IP Packets	Total number of IP packets received.
Rx IP Bytes	Total number of IP bytes received.
Tx CSTP Frames	Number of CSTP frames transmitted to the client.
Tx CSTP Bytes	Number of CSTP bytes (data plus control frames) transmitted to the client.
Tx CSTP Data Fr	Number of CSTP data frames transmitted to the client.
Tx CSTP CNTL Fr	Number of CSTP control frames transmitted to the client.
Tx CSTP DPD Req	Number of DPD requests transmitted from the gateway.
Tx CSTP DPD Res	Number of times the gateway processed a CSTP DPD request frame.
Tx Address Renew	Number of address renew requests transmitted at the gateway.
Tx CDTP Frames	Number of CDTP frames transmitted to the client.
Tx CDTP Bytes	Number of CDTP bytes transmitted to the client.
Tx CDTP Data Fr	Number of CDTP data frames transmitted to the client.
Tx CDTP CNTL Fr	Number of CDTP control frames transmitted to the client.
Tx CDTP DPD Req	Number of CDTP DPD requests transmitted to the gateway.
Tx CDTP DPD Res	Number of times the gateway processed a CDTP DPD request frame.
Tx IP Packets	Total number of IP packets transmitted.
Tx IP Bytes	Total number of IP bytes transmitted.
CEF Statistics	Cisco Express Forwarding statistics.

show webvpn sessions

Note Effective with Cisco IOS Release 12.4(6)T, the **show webvpn sessions** command is replaced by the **show webvpn session** command. See the **show webvpn session** command for more information.

To display information about WebVPN sessions, use the **show webvpn sessions** command in privileged EXEC mode.

show webvpn sessions

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(6)T	This command was replaced by the **show webvpn session** command.

Examples

The following output example displays information about a WebVPN session:

```
Router# show webvpn sessions

WebVPN domain name: cisco.com
Client Login Name          Client IP Address     Number of Connections
webuser                    172.16.163.142       4
    Created 00:14:25, Last-used 00:00:10
    Client Port: 2366
    Client Port: 2386
    Client Port: 2396
    Client Port: 2486
browseruser                172.16.163.142      2
    Created 00:00:09, Last-used 00:00:08
    Client Port: 2431
    Client Port: 2432
```

Table 212 describes the significant fields shown in the display

Table 212 show webvpn sessions Field Descriptions

Field	Description
Client Login Name	Username used to log in to the WebVPN gateway.
Client IP Address	IP address of the host from which the user is connecting.
Number of Connections	Number of active TCP connections by the user at this point.

Table 212 show webvpn sessions Field Descriptions (continued)

Field	Description
Created	Provides the time that has elapsed since the user logged in (in HH:MM:SS format).
Client Port	Local TCP port used on the client host.

Related Commands

Command	Description
show webvpn statistics	Displays WebVPN statistics.

show webvpn statistics

Note Effective with Cisco IOS Release 12.4(6)T, the **show webvpn statistics** command is replaced by the **show webvpn stats** command. See the **show webvpn stats** command for more information.

To display WebVPN statistics, use the **show webvpn statistics** command in privileged EXEC mode.

show webvpn statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(6)T	This command was replaced by the **show webvpn stats** command.

Examples

The following is sample output using the **show webvpn statistics** command:

```
Router# show webvpn statistics

Active user sessions: 2
Active user TCP connections: 6
Authentication failures: 3
Terminated user sessions: 0
```

Table 212 describes the significant fields shown in the display.

Table 213 show webvpn statistics Field Descriptions

Field	Description
Active user sessions	Number of users who are logged into the system.
Active user TCP connections	Number of TCP user connections that are used by the user session.
Authentication failures	Number of authentication failures to the gateway.
Terminated user sessions	Number of users who logged in and logged out after the statistics were cleared.

Related Commands

Command	Description
show webvpn sessions	Displays information about WebVPN sessions.

show webvpn stats

To display Secure Socket Layer Virtual Private Network (SSL VPN) application and network statistics, use the **show webvpn stats** command in privileged EXEC mode.

show webvpn stats [**cifs | citrix | mangle | port-forward | sso | tunnel**] [**detail**] [**context** {**all** | *name*}]

Syntax Description

cifs	(Optional) Displays Windows file share (Common Internet File System [CIFS]) statistics.
citrix	(Optional) Displays Citrix application statistics.
mangle	(Optional) Displays URL mangling statistics.
port-forward	(Optional) Displays port forwarding statistics.
sso	(Optional) Displays statistics for the Single SignOn (SSO) server.
tunnel	(Optional) Displays VPN tunnel statistics.
detail	(Optional) Displays detailed information.
context {**all** | *name*}	(Optional) Displays information for a specific context or all contexts.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(11)T	The **sso** keyword was added for Cisco 6500 Catalyst switches.
12.4(15)T	Output information was added for Cisco Express Forwarding (CEF).

Usage Guidelines

This command is used to display SSL VPN application, authentication, and network statistics and counters.

Examples

The following is sample output from the **show webvpn stats** command entered with the **detail** and **context** keywords:

```
Router# show webvpn stats detail context context1

WebVPN context name : context1
User session statistics:
    Active user sessions     : 0          AAA pending reqs         : 0
    Peak user sessions       : 0          Peak time                : never
    Active user TCP conns    : 0          Terminated user sessions : 0
    Session alloc failures   : 0          Authentication failures  : 0
    VPN session timeout      : 0          VPN idle timeout         : 0
    User cleared VPN sessions: 0          Exceeded ctx user limit  : 0
```

```
    CEF switched packets - client: 0          , server: 0
    CEF punted packets - client: 0          , server: 0

Mangling statistics:
    Relative urls             : 0          Absolute urls             : 0
    Non-http(s) absolute urls: 0           Non-standard path urls    : 0
    Interesting tags          : 0          Uninteresting tags        : 0
    Interesting attributes    : 0          Uninteresting attributes : 0
    Embedded script statement: 0           Embedded style statement  : 0
    Inline scripts            : 0          Inline styles             : 0
    HTML comments             : 0          HTTP/1.0 requests         : 0
    HTTP/1.1 requests         : 0          Unknown HTTP version      : 0
    GET requests              : 0          POST requests             : 0
    CONNECT requests          : 0          Other request methods     : 0
    Through requests          : 0          Gateway requests          : 0
    Pipelined requests        : 0          Req with header size >1K  : 0
    Processed req hdr bytes   : 0          Processed req body bytes  : 0
    HTTP/1.0 responses        : 0          HTTP/1.1 responses        : 0
    HTML responses            : 0          CSS responses             : 0
    XML responses             : 0          JS responses              : 0
    Other content type resp   : 0          Chunked encoding resp     : 0
    Resp with encoded content: 0           Resp with content length  : 0
    Close after response      : 0          Resp with header size >1K: 0
    Processed resp hdr size   : 0          Processed resp body bytes: 0
    Backend https response    : 0          Chunked encoding requests: 0

CIFS statistics:
  SMB related Per Context:
    TCP VC's                  : 0          UDP VC's                  : 0
    Active VC's               : 0          Active Contexts           : 0
    Aborted Conns             : 0
  NetBIOS related Per Context:
    Name Queries              : 0          Name Replies              : 0
    NB DGM Requests           : 0          NB DGM Replies            : 0
    NB TCP Connect Fails      : 0          NB Name Resolution Fails  : 0
  HTTP related Per Context:
    Requests                  : 0          Request Bytes RX          : 0
    Request Packets RX        : 0          Response Bytes TX         : 0
    Response Packets TX       : 0          Active Connections        : 0
    Active CIFS context       : 0          Requests Dropped          : 0

Socket statistics:
    Sockets in use            : 0          Sock Usr Blocks in use    : 0
    Sock Data Buffers in use  : 0          Sock Buf desc in use      : 0
    Select timers in use      : 0          Sock Select Timeouts      : 0
    Sock Tx Blocked           : 0          Sock Tx Unblocked         : 0
    Sock Rx Blocked           : 0          Sock Rx Unblocked         : 0
    Sock UDP Connects         : 0          Sock UDP Disconnects      : 0
    Sock Premature Close      : 0          Sock Pipe Errors          : 0
    Sock Select Timeout Errs  : 0

Port Forward statistics:
    Connections serviced      : 0            Server Aborts (idle)      : 0
  Client                                   Server
    in pkts                   : 0            out pkts                  : 0
    in bytes                  : 0            out bytes                 : 0
    out pkts                  : 0            in pkts                   : 0
    out bytes                 : 0            in bytes                  : 0

WEBVPN Citrix statistics:
Connections serviced : 0

                Server                    Client
  Packets in  : 0                          0
```

```
  Packets out : 0                          0
  Bytes in    : 0                          0
  Bytes out   : 0                          0

Tunnel Statistics:
    Active connections       : 0
    Peak connections         : 0          Peak time                : never
    Connect succeed          : 0          Connect failed           : 0
    Reconnect succeed        : 0          Reconnect failed         : 0
    SVCIP install IOS succeed: 0          SVCIP install IOS failed : 0
    SVCIP clear IOS succeed  : 0          SVCIP clear IOS failed   : 0
    SVCIP install TCP succeed: 0          SVCIP install TCP failed : 0
    DPD timeout              : 0
  Client                                 Server
    in  CSTP frames          : 0          out IP pkts              : 0
    in  CSTP data            : 0          out stitched pkts        : 0
    in  CSTP control         : 0          out copied pkts          : 0
    in  CSTP Addr Reqs       : 0          out bad pkts             : 0
    in  CSTP DPD Reqs        : 0          out filtered pkts        : 0
    in  CSTP DPD Resps       : 0          out non fwded pkts       : 0
    in  CSTP Msg Reqs        : 0          out forwarded pkts       : 0
    in  CSTP bytes           : 0          out IP bytes             : 0
    out CSTP frames          : 0          in  IP pkts              : 0
    out CSTP data            : 0          in  invalid pkts         : 0
    out CSTP control         : 0          in  congested pkts       : 0
    out CSTP Addr Resps      : 0          in  bad pkts             : 0
    out CSTP DPD Reqs        : 0          in  nonfwded pkts        : 0
    out CSTP DPD Resps       : 0          in  forwarded pkts       : 0
    out CSTP Msg Reqs        : 0
    out CSTP bytes           : 0          in  IP bytes             : 0
```

Table 214 describes significant fields in the **show webvpn stats detail context** display.

Table 214 show webvpn stats detail context Field Descriptions

Field	Description
WebVPN context name	Name of the context.
User session statistics:	
Active user sessions	Total number of currently active user sessions on the gateway.
Peak user sessions	Maximum number of simultaneous user sessions on the gateway since the gateway came up.
Active user TCP conns	Total number of currently active TCP connections that were initiated from the client side toward the SSL VPN gateway.
Session alloc failures	Total number of session allocation failures that were initiated from the client side. These failures occur because of a lack of memory on the gateway. Examples: • No free slot in session table • No memory for session allocation • No memory for gateway cookie allocation • Not enough memory on the gateway

Table 214 show webvpn stats detail context Field Descriptions (continued)

Field	Description
VPN session timeout	Information about the number of times the web VPN session timer has expired. This value reflects the full total for all the contexts that are configured at the gateway. The session timer is off by default, and it is enabled when an administrator intentionally uses the command-line interface (CLI) timeout session *number* argument under the **group policy** command submode.
User cleared VPN sessions	Total number of user-removed (or cleared) VPN sessions on the gateway. For example, if any user sessions are cleared using the CLI command **clear webvpn session** *user-name* **context** *context-name*, the counter is incremented by one.
AAA pending reqs	Total number of pending authentication, authorization, and accounting (AAA) requests on the gateway.
Peak time	Time elapsed since the peak number of simultaneous user sessions were observed on the gateway.
Terminated user sessions	Total number of expired user sessions on the gateway. Examples: • User logout sessions • Session cookie removed
Authentication failures	Total number of authentication failures on the gateway. Examples: • Wrong username and password • Empty username and password field
VPN idle timeout	Number of times the idle timer expired for all the contexts configured at the security gateway. Idle time refers to the time for which an active session can be left unattended (maximum time for which a session is up even though no traffic flows through the connection).
Exceeded ctx user limit	Total number of denied logins on the gateway that exceeded the context maximum user limit.
CEF switched packets (for client and server)	Packets that were CEF-switched.
CEF punted packets (for client and server)	Packets that could not be CEF-switched in a box with CEF switching enabled and that were “punted” to the next switching level.
Mangling statistics:	

Table 214 show webvpn stats detail context Field Descriptions (continued)

Field	Description
Relative urls	Number of URLs that point to a file/directory in relation to the present file/directory.
Non-http(s) absolute urls	Number of non-HTTP– relative URLs that are mangled.
Interesting tags	Number of HTTP, Cascade Style Sheets (CSS), or JavaScript tags that are mangled.
Interesting attributes	HTTP attributes, JavaScript, or CSS attributes that are mangled.
Embedded script statement	Embedded JavaScripts that were mangled.
Inline scripts	Number of inline CSSs that were mangled.
HTML comments	Number of HTML comments that were encountered.
HTTP/1.1 requests	Number of HTTP 1.1 requests that were encountered.
GET requests	Number of HTTP 1.0 or 1.1 GET requests that were encountered.
CONNECT requests	Number of HTTP 1.0 or 1.1 CONNECT requests that were encountered.
Pipelined requests	Number of requests dropped due to pipelines (pipelined requests are currently not supported).
Processed req hdr bytes	Total number of bytes in the requests made by the HTTP header to the backend server.
HTML /1.0 responses	Number of HTTP 1.0 responses that were encountered.
HTML responses	Total number of HTML pages that were received at the gateway.
XML responses	Total number of XML pages/responses that were received at the gateway.
Other content type resp	Total number of responses that were received other than HTML, XML, JavaScript, or CSS.
Resp with encoded content	Number of supported responses that were already encoded by the backend server.
Processed resp hdr size	Number of bytes in the headers of HTTP responses that were processed at the gateway.
Backend https response	Number of HTTP pages sent to the client by the backend server.
Absolute urls	Number of absolute HTTP URLs that were mangled.
Non-standard path urls	Number of non-HTTP–relative URLs that were mangled.
Uninteresting tags	HTTP attributes, JavaScript, or CSS attributes that were mangled.

Table 214 show webvpn stats detail context Field Descriptions (continued)

Field	Description
Uninteresting attributes	Number of attributes that were not mangled (for instance, XML attributes).
Embedded style statement	Embedded CSS and other styling sheets that were mangled.
Inline styles	Number of inline CSSs that were mangled.
HTTP/1.0 requests	Number of HTTP 1.0 requests that were encountered.
Unknown HTTP version	Number of HTTP version requests other than 1.0 and 1.1.
POST requests	Number of HTTP 1.0 or 1.1 POST requests that were encountered.
Other request methods	Number of non- (1.0 or 1.1) HTTP requests plus the number of requests other than GET, POST, or CONNECT.
Gateway requests	Number of requests made explicitly to the gateway.
Req with header size >1K	Number of requests to the backend server having a header size greater than 1024 bytes.
Processed req body bytes	Total number of bytes processed while parsing HTML requests (body means the total bytes processed or read in an HTML request excluding the header).
HTTP/1.1 responses	Number of HTTP 1.1 responses that were received at the gateway.
CSS responses	Total number of CSS tags that were received.
JS responses	Total number of JavaScript responses that were received at the gateway.
Chunked encoding resp	Number of times transfer encoding was set to “chunked” in an HTTP response.
Resp with content length	Number of non-zero content-length responses.
Resp with header size > 1K	Responses received at the gateway with a header size greater than 1 kilobyte.
Processed resp body bytes	Total number of bytes that were processed in responses (number of bytes in the bodies of the messages).
Chunked encoding requests	Number of requests that were chunk encoded.
CIFS statistics:	
SMB related Per Context:	
TCP VC’s	Backend TCP connections established successfully (thus far).
Active VC’s	Currently active TCP/User Datagram Protocol (UDP) connections.

Table 214 show webvpn stats detail context Field Descriptions (continued)

Field	Description
Aborted Conns	Number of TCP-aborted connections (thus far).
UDP VC's	Backend TCP connections established successfully (thus far).
Active Contexts	Currently active Server Message Block (SMB) contexts.
NetBIOS related Per Context:	
Name Queries	NetBIOS name service (NBNS) name queries that have been sent.
NB DGM Requests	NetBios datagram service-related GET backup browser-list queries that have been sent.
NB TCP Connect Fails	NetBios TCP connections that failed.
Name Replies	NBNS name-query replies that have been received. Mismatch indicates that browsers/primary domain controller (PDC)/servers could not be contacted.
NB DGM Replies	NetBIOS datagram service-related GET backup browser replies were received. Request/reply mismatch indicates that a browse domain attempt would not work.
NB Name Resolution Fails	NetBIOS name resolution requests sent to the PDC failed.
HTTP related Per Context:	
Requests	Number of HTTP requests made per a CIFS application context.
Request Packets RX	Number of HTTP packets received per a CIFS application context.
Response Packets TX	Number of HTTP packets sent per a CIFS application context.
Active CIFS context	Number of active CIFS application module contexts on which CIFS requests are being processed.
Request Bytes RX	Number of HTTP bytes received per a CIFS application context.
Response Bytes TX	Number of HTTP bytes sent per a CIFS application context.
Active Connections	Number of active CIFS connections.
Requests Dropped	Number of HTTP requests dropped per CIFS application context.
Socket statistics:	
Sockets in use	Number of sockets that are in use by SSL VPN socket layer.

Table 214 show webvpn stats detail context Field Descriptions (continued)

Field	Description
Sock Data Buffers in use	Number of data buffers that are used by the socket layer.
Select timers in use	Number of socket select timers that are in use.
Sock TX Blocked	Number of times an application send was blocked by TCP congestion control.
Sock Rx Blocked	Number of times an application blocked further reception of data from the TCP layer. The blocking indicates application buffer starvation or a processing limit.
Sock UDP Connects	Number of UDP connects to the gateway.
Sock Premature Close	Number of times an application received a Closed connection before it could be established.
Sock Select Timeout Errs	Number of times a socket select timeout error occurred.
Sock Usr Blocks in use	Number of user blocks in use.
Sock Buf desc in use	Number of socket buffer descriptors in use.
Sock Select Timeouts	Number of times an application timed out while waiting for a reply in a request/reply exchange or while waiting for a TCP connection to be established.
Sock Tx Unblocked	Number of times an application send resumed after being blocked due to TCP congestion control. If the transmit blocked and unblocked do not match after a sufficient period of time, the transaction is stalled.
Sock Rx Unblocked	Number of times an application resumed further reception of data from the TCP layer. If receive blocked and unblocked do not match after a sufficient period of time, the transaction is stalled.
Sock UDP Disconnects	Number of UDP disconnects to the gateway.
Sock Pipe Errors	Number of times socket pipe establishment failed.
WEBVPN Citrix statistics:	
Server	
Packets in	Number of packets received from the server.
Packets out	Number of packets sent to the server.
Bytes in	Number of bytes received from the server.
Bytes out	Number of bytes sent to the server.
Client	
Packets in	Number of packets received from the client.
Packets out	Number of packets sent to the client.
Bytes in	Number of bytes received from the server.

Table 214 show webvpn stats detail context Field Descriptions (continued)

Field	Description
Bytes out	Number of bytes sent to the client.
Tunnel Statistics:	
Active connections	Number of active tunnels.
Peak connections	Maximum number of simultaneously active tunnels as observed since the last reboot of the Cisco IOS router or last counter reset.
Connect succeed	Number of tunnel connections that have succeeded since the last reboot of the Cisco IOS router or last counter reset.
Reconnect succeed	Number of tunnel connections that have succeeded in reconnecting since the last reboot of the Cisco IOS router or last counter reset.
SVCIP install IOS succeed	Number of times, during the SSL VPN Client (SVC)/AnyConnect package installation, that the frame IP address or allocated IP address is used (IP address sticky).
SVCIP clear IOS succeed	Number of times an SVC IP address is successfully removed from the IP alias on the core.
SVCIP install TCP succeed	Number of tunnel connections that have succeeded since the last reboot of the Cisco IOS router or last counter reset.
DPD timeout	Number of Dead Peer Detection (DPD) timeout sessions.
Peak time	Absolute timestamp when the peak full-tunnel connections were observed.
Connect failed	Number of tunnel connections that have failed since the last reboot of the Cisco IOS router or last counter reset.
Reconnect failed	Number of tunnel connections that have failed in reconnecting since the last reboot of the Cisco IOS router or last counter reset.
SVCIP install IOS failed	Total number of times, during the SVC/AnyConnect installation, that an IP assignment from the pool fails or failed to configure an IP address to the virtual route forwarding (VRF) table.
SVCIP clear IOS failed	Number of times an STC IP address could not be removed from the IP alias on the core.
SVCIP install TCP failed	Number of tunnel connections that have failed since the last reboot of the Cisco IOS router or last counter reset.
Client	

Table 214 show webvpn stats detail context Field Descriptions (continued)

Field	Description
in CSTP frames	Number of Cisco SSL Tunnel Protocol (CSTP) frames from the client.
in CSTP data	Number of CSTP data frames from the client.
in CSTP control	Number of CSTP control frames from the client.
in CSTP Addr Reqs	Number of IP address renewal requests received by the gateway.
in CSTP DPD Reqs	Number of DPD requests received at the gateway.
in CSTP DPD Resps	Number of DPD responses received at the gateway (The client sends the DPD requests, the gateway responds to the transmission, and the client responds back. It is this response that is counted here.)
in CSTP Msg Reqs	Number of times a CSTP message control frame is received at the gateway.
in CSTP bytes	Number of CSTP bytes (data+control frames) from the client.
out CSTP frames	Number of CSTP frames to the client.
out CSTP data	Number of CSTP data frames to the client.
out CSTP control	Number of CSTP control frames to the client.
out CSTP DPD Reqs	Number of times at-gateway CSTP control frames were generated.
out CSTP DPD Resps	Number of times the gateway processed a CSTP DPD request frame.
out CSTP Msg Reqs	Number of times the gateway generated a CSTP message (MSG) frame.
out CSTP bytes	Number of CSTP bytes (data+control frames) to the client.
Server	
out IP pkts	IP datagrams that are successfully forwarded to the server.
out bad pkts	Number of times a bad tunneled IP packet was dropped at the gateway.
out filtered pkts	Number of times a tunneled IP packet was dropped at the gateway due to a named or numbered ACL that was configured at the gateway.
out non fwded pkts	Number of times a tunneled IP packet could not be forwarded due to routing issues.
out forwarded pkts	Number of times a tunneled IP packet was successfully forwarded by the gateway.
out IP bytes	IP datagram bytes that are successfully forwarded to the server.

Table 214 show webvpn stats detail context Field Descriptions (continued)

Field	Description
in IP pkts	IP datagrams that are successfully received from the server.
in IP bytes	IP datagram bytes that are successfully received from the server.

The following example displays SSO statistics:

```
Router# show webvpn stats sso

   Auth Requests             : 4          Pending Auth Requests      : 0
   Successful Requests       : 1          Failed Requests            : 3
   Retranmissions            : 0          DNS Errors                 : 0
   Connection Errors         : 0          Request Timeouts           : 0
   Unknown Responses         : 0
```

Table 215 describes significant fields in the **show webvpn stats sso** display.

Table 215 show webvpn stats sso Field Descriptions

Field	Description
Auth Requests	Number of SSO authentication requests.
Successful Requests	Number of SSO authentication requests that passed successfully.
Retransmissions	Total number of times authentication requests were resent for authentication. The resending occurs when the SSO timer expires and no response is received from the SSO server for authentication requests.
Connection Errors	Number of failures to sign on to the SSO server.
Unknown Responses	Number of times an SSO authentication request yielded results other than failure or success (includes errors, such as access control list [ACL] errors).
Pending Auth Requests	Total number of SSO authentication requests pending to be processed for authentication.
Failed Requests	Number of times SSO authentication failed.
DNS Errors	Number of times an SSO server could not be resolved.
Request Timeouts	Number of times an SSO authentication request timed out.

The following example displays information about CEF:

```
Router# show webvpn stats

User session statistics:
   Active user sessions      : 1          AAA pending reqs          : 0
```

```
  Peak user sessions       : 1           Peak time                : 00:12:01
  Active user TCP conns    : 1           Terminated user sessions : 1
  Session alloc failures   : 0           Authentication failures  : 0
  VPN session timeout      : 0           VPN idle timeout         : 0
  User cleared VPN sessions: 0           Exceeded ctx user limit  : 0
  Exceeded total user limit: 0
  Client process rcvd pkts : 37          Server process rcvd pkts : 0
  Client process sent pkts : 1052        Server process sent pkts : 0
  Client CEF received pkts : 69          Server CEF received pkts : 0
  Client CEF rcv punt pkts : 1           Server CEF rcv punt pkts : 0
  Client CEF sent pkts     : 1102        Server CEF sent pkts     : 0
  Client CEF sent punt pkts: 448         Server CEF sent punt pkts: 0

  SSLVPN appl bufs inuse   : 0           SSLVPN eng  bufs inuse   : 0
Active server TCP conns    : 0
```

Table 216 describes fields in the **show webvpn stats** display.

Table 216 show webvpn stats Field Descriptions

Field	Description
User session statistics:	
Active user sessions	Total number of currently active user sessions on the gateway.
Peak user sessions	Maximum number of simultaneous user sessions on the gateway since the gateway came up.
Active user TCP conns	Total number of currently active TCP connections that were initiated from the client side toward the SSL VPN gateway.
Session alloc failures	Total number of session allocation failures that were initiated from the client side. These failures occur because of a lack of memory on the gateway. Examples: • No free slot in session table • No memory for session allocation • No memory for gateway cookie allocation Not enough memory on the gateway
VPN session timeout	Information about the number of times the web VPN session timer has expired. This value reflects the full total for all the contexts that are configured at the gateway. The session timer is OFF by default, and it is enabled when an administrator intentionally uses the CLI timeout session *number* argument under the **group policy** command submode.

Table 216 show webvpn stats Field Descriptions (continued)

Field	Description
User cleared VPN sessions	Total number of user-removed (or cleared) VPN sessions on the gateway. For example, if any user sessions are cleared using the CLI command **clear webvpn session** *user-name* **context** *context-name*, the counter is incremented by one.
Exceeded total user limit	Total number of denied logins on the gateway. An SSL VPN gateway can support the maximum user sessions (up to 1000).
Client process rcvd pkts	Total number of packets that were received from the client on the SSL VPN gateway.
Client process sent pkts	Total number of data packets that were sent to the client side from the SSL VPN gateway.
Client CEF received pkts	Total number of CEF-related packets that were received from the client on the gateway.
Client CEF rcv punt pkts	Total number of punt packets that were received from the client on the gateway. Punting is defined as the handling of CEF-intended data on the slower path (called the process path). Punting occurs when the data is not handled by the CEF path. Example: • If any control packets are received on the CEF path, those packets will punt to the slower path (process path), which is not handled by the CEF path.
Client CEF sent pkts	Total number of data packets that were sent via the CEF path to the client side from the gateway.
Client CEF sent punt pkts	Total number of punt packets (data sent via a slow path) that were sent to the client from the gateway.
SSLVPN appl bufs inuse	Total number of buffers that are allocated for data or application processing on the gateway.
Active server TCP conns	Total number of currently active TCP connections on the gateway that were initiated from the server side toward the SSL VPN gateway.
AAA pending reqs	Total number of pending AAA requests on the gateway.
Peak time	Time elapsed since the peak number of simultaneous user sessions were observed on the gateway.

Table 216 show webvpn stats Field Descriptions (continued)

Field	Description
Terminated user sessions	Total number of expired user sessions on the gateway. Examples: • User logout sessions • Session cookie removed
Authentication failures	Total number of authentication failures on the gateway. Examples: • Wrong username and password • Empty username and password field
VPN idle timeout	Number of times the idle timer expired for all the contexts configured at the security gateway. Idle time refers to the time for which an active session can be left unattended (maximum time for which a session is up even though no traffic flows through the connection).
Exceeded ctx user limit	Total number of denied logins on the gateway that exceeded the context maximum user limit.
Server process rcvd pkts	Total number of control packets that were received from the server side of the SSL VPN gateway.
Server process sent pkts	Total number of control packets that were sent to the server side from the SSL VPN gateway.
Server CEF received pkts	Total number of data CEF-related packets that were received from the server side of the SSL VPN gateway.
Server CEF rcv punt pkts	Total number of punt packets that were received from the server on the SSL VPN gateway.
Server CEF sent pkts	Total number of data (CEF-related) packets that were sent to the server from the SSL VPN gateway.
Server CEF sent punt pkts	Total number of punt packets that were sent to the server side from the SSL VPN gateway.
SSLVPN eng bufs inuse	Total number of buffers that were allocated for engine processing on the gateway.

Related Commands

Command	Description
clear webvpn stats	Clears application and access counters on an SSL VPN gateway.

show wlccp wds

To display information either about the wireless domain services (WDS) device or about client devices, use the **show wlccp wds** command in privileged EXEC mode.

show wlccp wds [**ap | mn**] [**detail**] [**mac-addr** *mac-address*]

Syntax Description

ap	(Optional) Displays access points participating in Cisco Centralized Key Management.
mn	(Optional) Displays cached information about client devices, also called mobile nodes.
detail	(Optional) Displays the lifetime of the client, the service set identifier (SSID), and the virtual VLAN ID.
mac-addr	(Optional) Displays information about a specific client device.
mac-address	Client's MAC address.

Defaults

If you do not enter any options with the **show wlccp wds** command, this command displays the IP address of the WDS device, the MAC address, the priority, and the interface state. If the interface state is backup, the command also displays the IP address of the current WDS device, the MAC address, and the priority.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)JA	This command was introduced.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

To show information about the WDS device, do not enter any keywords with this command.

Examples

The following command entry displays information about the WDS device:

```
Router# show wlccp wds ap
```

The following command entry displays cached information, including details, about the client device with the specified MAC address:

```
Router# show wlccp wds mn detail mac-addr 00-05-C2-00-01-F5
```

The following is sample output from the **show wlccp wds** command:

```
Router# show wlccp wds

      MAC:0001.28e0.a400, IP-ADDR:10.0.0.1       , Priority:255
      Interface Vlan1, State:Administratively StandAlone - ACTIVE
      AP Count:1    , MN Count:0    , MAX AP Count:50
```

Table 217 describes the significant fields shown in the display.

Table 217 show wlccp wds Field Descriptions

Field	Description
MAC	MAC address of the interface on which the WDS is configured.
IP-ADDR	IP address of the interface on which the WDS is configured.
Priority	Priority of the WDS.
Interface	Interface on which the WDS is configured.
State	State of the WDS. The state can be INITIALIZATION, BACKUP, or ACTIVE.
AP Count	Number of access points registered to the WDS.
MN Count	Number of mobile nodes registered to the WDS.
MAX AP Count	Maximum number of access points that can be registered.

Related Commands

Command	Description
debug wlccp packet	Displays packet traffic to and from the WDS router.
debug wlccp wds	Displays either WDS debug state or WDS statistics messages.
wlccp authentication-server client	Configures the list of servers to be used for 802.1X authentication.
wlccp authentication-server infrastructure	Configures the list of servers to be used for 802.1X authentication for the wireless infrastructure devices.
wlccp wds priority interface	Enables a wireless device such as an access point or a wireless-aware router to be a WDS candidate.

show zone security

To display zone security information, use the **show zone security** command in user EXEC or privileged EXEC mode.

show zone security [*security-zone-name*]

Syntax Description

security-zone-name	(Optional) The security zone name.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.
Cisco IOS 2.1 XE	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use this command to display zone security information.

Examples

The following is sample output from the **show zone security** command. The fields are self-explanatory.

```
Router# show zone security

zone self
Description: System defined zone
```

show zone-pair security

To display the source zone, destination zone, and policy attached to the zone-pair, use the **show zone-pair security** command in privileged EXEC mode. To disable the display, use the **no** form of this command.

show zone-pair security [**source** *source-zone-name*] [**destination** *destination-zone-name*]

no show zone-pair security [**source** *source-zone-name*] [**destination** *destination-zone-name*]

Syntax Description

source *source-zone-name*	(Optional) Name of the source zone.
destination *destination-zone-name*	(Optional) Name of the destination zone.

Command Default

If you do not specify a source or destination zone, the system displays all the zone-pairs for the source, destination, and the associated policy.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following example displays the source zone, destination zone, and policy attached to the zone-pair:

```
Router# show zone-pair security source z1 destination z2

zone-pair name zp
  Source-Zone z1  Destination-Zone z2
  service-policy p1
```

Table 218 describes the significant fields shown in the display.

Table 218 show zone-pair security Field Descriptions

Field	Description
zone-pair name	Name of the zone-pair.
Source-Zone	Name of the source zone.
Destination-Zone	Name of the destination zone.
service-policy	Name of the service policy.

shutdown (firewall)

To shut down a group manually, use the **shutdown** command in redundancy application group configuration mode**.** To enable a redundancy group, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

The group is active.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

When a group is shut down, it does not participate in the role negotiation. The group remains in the shutdown state until you execute the **no shutdown** command.

Examples

The following example shows how to shut down a group named group1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# shutdown
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.

shutdown (certificate server)

To allow a certificate server to be disabled without removing the configuration, use the **shutdown** command in certificate server configuration mode. To reenable the certificate server, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

no shutdown

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

You should issue the **no shutdown** command only after you have completely configured your certificate server.

The **shutdown** command disables the certificate server. If you prefer to disable simple certificate enrollment protocol (SCEP) but still want the certificate server for manual certificate enrollment, use the **no ip http server** command.

Examples

To ensure that the specified URL is working correctly, configure the **database url** command before you issue the **no shutdown** command on the certificate server for the first time. If the URL is broken, you will see output as follows:

```
Router(config)# crypto pki server mycs
Router(cs-server)# database url ftp://myftpserver
Router(cs-server)# no shutdown
% Once you start the server, you can no longer change some of
% the configuration.
Are you sure you want to do this? [yes/no]: yes
Translating "myftpserver"

% Failed to generate CA certificate - 0xFFFFFFFF
% The Certificate Server has been disabled.
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters PKI configuration mode.
database url	Specifies the location where all database entries for the certificate server will be written out.
ip http server	Enables an HTTP server on your network.

signature

To specify a signature for which the command-line interface (CLI) user tunings will be changed, use the **signature** command in signature-definition-signature (config-sigdef-sig) configuration mode. To remove the CLI user tunings and rev**e**rt to the default values, use the **no** version of this command.

signature *signature-id* [*subsignature-id*]

no signature *signature-id* [*subsignature-id*]

Syntax Description

signature-id [*subsignature-id*]	Signature number. If a subsignature is not specified, the default is 0. For example, if signature 1105 is specified without a subsignature, the router will interpret the signature as 1105:0.

Command Default

Default signature parameters cannot be changed.

Command Modes

Signature-definition-signature configuration (config-sigdef-sig)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use the **signature** command to specify a signature whose CLI user tunings are to be customized. Thereafter, you can begin to specify which signature parameters (user tunings) are to be changed.

Examples

The following example shows how to modify signature 5081/0 to “produce alert” and “reset tcp connection”:

```
Router(config)# ip ips signature-definition
Router(config-sigdef-sig)# signature 5081 0
Router(config-sigdef-action)# engine
Router(config-sigdef-action-engine)# event-action produce-alert reset-tcp-connection
Router(config-sigdef-action-engine)# ^Z
Do you want to accept these changes:[confirmm]y
```

Related Commands

Command	Description
ip ips signature-definition	Enters signature-definition-signature configuration mode, which allows you to define a signature for CLI user tunings.

smart-tunnel list

To configure the smart tunnel list and enable it within a policy group, use the **smart-tunnel list** command in WebVPN context configuration mode or WebVPN group policy configuration mode. To disable the smart tunnel configuration, use the **no** form of this command.

smart-tunnel list *name*

no smart-tunnel list

Syntax Description

name	Smart tunnel list name.

Command Default

No smart tunnel list is created and enabled.

Command Modes

WebVPN context configuration mode (config-webvpn-context)
WebVPN group policy configuration mode (config-webvpn-group)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Before a smart tunnel list can be enabled within a group policy, it must be created. Applications that are to be directed to the smart tunnel then must be specified within the list. This list must later be applied to the group policy.

Note To remove a smart tunnel list, first use the **no smart-tunnel list** command in WebVPN group policy configuration mode, and then use the **no smart-tunnel list** command in WebVPN context configuration mode.

Examples

The following example shows how to create a smart tunnel list named “st1” and configure the applications for smart tunneling:

```
Router(config)# webvpn context sslgw
Router(config-webvpn-context)# smart-tunnel list st1
Router(config-webvpn-smart-tunnel)# appl ie ieexplore.exe windows
Router(config-webvpn-smart-tunnel)# appl telnet telnet.exe windows
```

The following example shows how to enable the smart tunnel list “st1” within a group policy:

```
Router(config)# webvpn context sslgw
Router(config-webvpn-context)# policy group new
Router(config-webvpn-group)# smart-tunnel list st1
```

Related Commands

Command	Description
webvpn context	Configures the SSL VPN context.
app (webvpn)	Configures applications to access smart tunnel.

snmp-server enable traps ipsec

To enable the router to send IP Security (IPSec) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps ipsec** command in global configuration mode. To disable IPSec SNMP notifications, use the **no** form of this command.

snmp-server enable traps ipsec [**cryptomap** [**add** | **delete** | **attach** | **detach**] | **tunnel** [**start** | **stop**] | **too-many-sas**]

no snmp-server enable traps ipsec [**cryptomap** [**add** | **delete** | **attach** | **detach**] | **tunnel** [**start** | **stop**] | **too-many-sas**]

Syntax Description

cryptomap add	(Optional) Notifications for cipsCryptomapAdded { cipsMIBNotifications 3 } events are generated, as defined in the CISCO-IPSEC-MIB. These notifications are generated when a new cryptomap is added to the specified cryptomap set.
cryptomap delete	(Optional) Notifications for cipsCryptomapDeleted { cipsMIBNotifications 4 } events are generated, as defined in the CISCO-IPSEC-MIB. These notifications are generated when a cryptomap is removed from the specified cryptomap set.
cryptomap attach	(Optional) Notifications for cipsCryptomapSetAttached { cipsMIBNotifications 5 } events are generated, as defined in the CISCO-IPSEC-MIB. These notifications are generated when a cryptomap set is attached to an active interface of the managed entity.
cryptomap detach	(Optional) Notifications for cipsCryptomapSetDetached { cipsMIBNotifications 6 } events are generated, as defined in the CISCO-IPSEC-MIB. These notifications are generated when a cryptomap set is detached from an interface to which it was previously bound.
tunnel start	(Optional) Notifications for cipSecTunnelStart { cipSecMIBNotifications 7 } events are generated, as defined in the CISCO-IPSEC-FLOW-MONITOR-MIB. These notifications are generated when an IPsec Phase-2 Tunnel becomes active.
tunnel stop	(Optional) Notifications for cipSecTunnelStop { cipSecMIBNotifications 8 } events are generated, as defined in the CISCO-IPSEC-FLOW-MONITOR-MIB. These notifications are generated when an IPsec Phase-2 Tunnel becomes inactive.
too-many-sas	(Optional) Notifications for cipsTooManySAs { cipsMIBNotifications 7 } events are generated, as defined in the CISCO-IPSEC-MIB.my. These notifications are generated when an attempt to make a new security association (SA) is made but there is insufficient memory on the device.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.1(11b)E	This command was integrated into Cisco IOS Release 12.1(11b)E.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

A cryptomap is a table that maps an IPSec Phase-2 tunnel to the corresponding IPSec Policy element.

For a complete description of the notification types and additional MIB functions, refer to the CISCO-IP-SEC.my and CISCO-IPSEC-FLOW-MONITOR-MIB.my files, available on Cisco.com through:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

The **snmp-server enable traps ipsec** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

In the following example, the router is configured to send IPSec MIB inform notifications to the host nms.cisco.com using the community string named “public”:

```
snmp-server enable traps ipsec
snmp-server host nms.cisco.com informs public ipsec
```

Related Commands

Command	Description
snmp-server enable traps isakmps	Controls the sending of (ISAKMP) SNMP notifications
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps isakmp

To enable the router to send IP Security (IPSec) Internet Security Association and Key Exchange Protocol (ISAKMP) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps isakmp** command in global configuration mode. To disable ISAKMP IPSec SNMP notifications, use the **no** form of this command.

snmp-server enable traps isakmp [**policy** {**add** | **delete**} | **tunnel** {**start** | **stop**}]

no snmp-server enable traps isakmp [**policy** {**add** | **delete**} | **tunnel** {**start** | **stop**}]

Syntax Description

policy add	(Optional) Notifications for cipsIsakmpPolicyAdded { cipsMIBNotifications 1 } events are generated, as defined in the CISCO-IPSEC-MIB. These notifications are generated when a new ISAKMP policy element is defined on the managed entity. The context of the event includes the updated number of ISAKMP policy elements currently available.
policy delete	(Optional) Notifcations for cipsIsakmpPolicyDeleted { cipsMIBNotifications 2 } events are generated, as defined in the CISCO-IPSEC-MIB. These notifications are generated when an existing ISAKMP policy element is deleted on the managed entity. The context of the event includes the updated number of ISAKMP policy elements currently available.
tunnel start	(Optional) Notifications for cikeTunnelStart { cipSecMIBNotifications 1 } events are generated, as defined by in the CISCO-IPSEC-FLOW-MONITOR-MIB.my. These notifications are generated when an IPsec Phase-1 IKE Tunnel becomes active.
tunnel stop	(Optional) Notifications for cikeTunnelStop { cipSecMIBNotifications 2 } events are generated, as defined by in the CISCO-IPSEC-FLOW-MONITOR-MIB.my. These notifications are generated when an IPsec Phase-1 IKE Tunnel becomes inactive.

Defaults

SNMP notifications are disabled by default.

If no keywords are specified, all available ISAKMP traps are enabled (or disabled if the **no** form is used).

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.1(11b)E	This command was integrated into Cisco IOS Release 12.1(11b)E
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both ISAKMP trap and inform requests.

For a complete description of these notifications and additional MIB functions, refer to the CISCO-IPSEC-MIB.myand CISCO-IPSEC-FLOW-MONITOR-MIB.my files, available on Cisco.com through:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

The **snmp-server enable traps isakmp** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

In the following example, the router is configured to send IPSec MIB inform notifications to the host nms.cisco.com using the community string named “public”:

```
snmp-server enable traps isakmp
snmp-server host nms.cisco.com informs public ipsec
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps nhrp

To enable Simple Network Management Protocol (SNMP) notifications for the Next Hop Resolution Protocol (NHRP), use the **snmp-server enable traps nhrp** command in global configuration mode. To disable SNMP NHRP notifications, use the **no** form of this command.

snmp-server enable traps nhrp [**nhc** [**down** | **up**] | **nhp** [**down** | **up**] | **nhs** [**down** | **up**] | **quota-exceeded**]

no snmp-server enable traps nhrp [**nhc** [**down** | **up**] | **nhp** [**down** | **up**] | **nhs** [**down** | **up**] | **quota-exceeded**]

Syntax Description

nhc	(Optional) Enables Next Hop Client (NHC) notifications.
down	(Optional) Enables notifications for when the client, peer, or server interface is declared 'down'.
up	(Optional) Enables notifications for when the client, peer, or server interface is declared 'up'.
nhp	(Optional) Enables Next Hop Peer (NHP) notifications.
nhs	(Optional) Enables Next Hop Server (NHS) notifications.
quota-exceeded	(Optional) Enables notifications for when the rate limit set on NHRP packets is exceeded on the interface.

Command Default

No notifications (traps) are enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

By default all notifications (traps) are disabled. You must explicitly enable any notifications that you need in your system. After you enable traps in your system, you can use the **snmp-server host traps** command to control which traps are sent to a particular trap receiver.

The **snmp-server host traps nhrp** command enables the default NHRP traps only (it does not enable all NHRP traps). The default traps include the NHS, NHC, and quota-exceeded traps.

Examples

The following example shows how to enable the default NHRP traps, and how to send these NHRP traps to the notification receiver with the IP address 192.40.3.130 using the community string public:

```
Router(config)# snmp-server enable traps nhrp
Router(config)# snmp-server host 192.40.3.130 traps version 2c public nhrp
```

The following example shows how to disable NHC traps and enable rate limit traps:

```
Router(config)# no snmp-server enable traps nhrp nhc
Router(config)# snmp-server enable traps nhrp quota-exceeded
```

Related Commands

Command	Description
debug snmp mib nhrp	Displays messages about the SNMP NHRP MIB.
snmp-server host	Specifies the recipient of an SNMP notification operation.

snmp trap ip verify drop-rate

To configure the router to send a Simple Network Management Protocol (SNMP) notification when the Unicast Reverse Path Forwarding (RPF) drop rate exceeds the configured threshold, use the **snmp trap ip verify drop-rate** command in interface configuration mode. To disable SNMP notification, use the **no** form of this command.

snmp trap ip verify drop-rate

no snmp trap ip verify drop-rate

Syntax Description

This command has no arguments or keywords.

Command Default

No SNMP notifications are sent.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI2	This command was integrated into Cisco IOS Release 12.2(33)SXI2.

Usage Guidelines

This command enables cipUrpfIfDropRateNotify notification. This notification is sent when the Unicast RPF drop rate exceeds the threshold.

Examples

The following example shows how to configure SNMP notification for the Unicast RPF drop rate on Ethernet interface 3/0:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 3/0
Router(config-if)# snmp trap ip verify drop-rate
```

Related Commands

Command	Description
ip verify drop-rate compute window	Configures the interval of time over which the Unicast RPF drop count used in the drop rate computation is collected.
ip verify unicast notification threshold	Configures the Unicast RPF drop count threshold which, when exceeded, triggers a notification.

source interface

To specify the address of an interface to be used as the source address for all outgoing TCP connections associated with a trustpoint, use the **source interface** command in ca-trustpoint configuration mode. To disable the interface that was specified, use the **no** form of this command.

source interface *interface-name*

no source interface *interface-name*

Syntax Description

interface-name	Interface address to be used as the source address for all outgoing TCP connections associated with a trustpoint.

Defaults

If this command is not specified, the address of the outgoing interface is used.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.

Usage Guidelines

This command must be used following the **crypto ca trustpoint** command. If this command is used and the address of the outgoing interface is specified, the router uses the specified address (or address of the specified interface) as the source address for any datagrams that are sent to the certification authority (CA) server or Lightweight Directory Access Protocol (LDAP) server during authentication, enrollment, and if appropriate, when obtaining certificate revocation lists (CRLs).

Examples

In the following example, the router is located in a branch office. The router uses IP Security (IPSec) to communicate with the main office. Ethernet 1 is the "outside" interface that connects to the Internet Service Provider (ISP). Ethernet 0 is the interface connected to the LAN of the branch office. To access the CA server located in the main office the router needs to send its IP datagrams out interface Ethernet 1 (address 10.2.2.205) using the IPSec tunnel. Address 10.2.2.205 is assigned by the ISP. Address 10.2.2.205 is not a part of the branch office or main office.

The CA cannot access any address outside the company because of a firewall. The CA sees a message coming from 10.2.2.205 and cannot respond (that is, it does not know that the router is located in a branch office at address 10.1.1.1, which it is able to reach).

Adding the **source interface** command tells the router to use address 10.1.1.1 as the source address of the IP datagram that it sends to the CA. The CA is able to respond to 10.1.1.1.

This scenario is configured using the **source interface** command and the interface addresses as described above.

```
crypto ca trustpoint ms-ca
 enrollment url http://yourname:80/certsrv/mscep/mscep.dll
 source interface ethernet0
!
interface ethernet 0
 description inside interface
 ip address 10.1.1.1 255.255.255.0
!
interface ethernet 1
 description outside interface
 ip address 10.2.2.205 255.255.255.0
 crypto map main-office
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

source interface (Diameter peer)

To configure the interface to be used for the Diameter peer connection, use the **source interface** command in Diameter peer configuration mode. To disable the interface configuration, use the **no** form of this command.

source interface {*interface*}

no source interface {*interface*}

Syntax Description

interface	Source address and port that initiate the TCP connection to the peer.

Command Default

No source interface is defined.

Command Modes

Diameter peer configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

The Diameter client uses the configured source address and port to initiate a TCP connection to the Diameter peer.

Examples

The following example shows how to configure a source address and port on the Diameter client:

```
Router (config-dia-peer)# source interface interface_01
```

Related Commands

Command	Description
diameter peer	Configures a Diameter peer and enters Diameter peer configuration submode.
show diameter peer	Displays the Diameter peer configuration.

source-interface (URL parameter-map)

To specify the interface whose IP address will be used as the source IP address while making a TCP connection to the URL filter server, use the **source-interface** command in URL parameter-map configuration mode. To stop using the IP address of the specified interface, use the **no** form of this command.

source-interface *interface-name*

no source-interface *interface-name*

Syntax Description

interface-name	Name of the interface.

Command Default

None

Command Modes

URL parameter-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

When you are creating or modifying a URL parameter map, you can enter the **source-interface** subcommand after you enter the **parameter-map type urlfilter** command.

Examples

The following example specifies that the IP address of Ethernet0 will be used as the source IP address while making a TCP connection to the URL filter server:

```
parameter-map type urlfilter u1
 source-interface ethernet0
```

Related Commands

Command	Description
parameter-map type urlfilter	Creates or modifies a parameter map for URL filtering parameters

split-dns

To specify a domain name that must be tunneled or resolved to the private network, use the **split-dns** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove a domain name, use the **no** form of this command.

split-dns *domain-name*

no split-dns *domain-name*

Syntax Description

domain-name	Name of the Domain Name System (DNS) domain that must be tunneled or resolved to the private network.

Defaults

All domain names are resolved via the public DNS server.

Command Modes

ISAKMP group configuration (config-isakmp-group)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

If you configure the **split-dns** command, the split-dns attribute will be added to the policy group. The attribute will include the list of domain names that you configured. All other names will be resolved via the public DNS server.

You must enable the **crypto isakmp client configuration group** command, which specifies group policy information that needs to be defined or changed, before enabling the **split-dns** command.

Note If you have to configure more than one domain name, you have to add a **split-dns** command line for each.

Examples

The following example shows that the domain names “green.com” and “acme.org” will be added to the policy group:

```
Router (config)# crypto isakmp client configuration group cisco
Router (config-isakmp-group)# key cisco
Router (config-isakmp-group)# dns 10.2.2.2 10.2.2.3
Router (config-isakmp-group)# wins 10.6.6.6
Router (config-isakmp-group)# domain cisco.com
Router (config-isakmp-group)# pool green
Router (config-isakmp-group)# acl 199
Router (config-isakmp-group)# split-dns green.com
```

```
Router (config-isakmp-group)# split-dns acme.org
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto isakmp client configuration group	Specifies group policy information that needs to be defined or changed.

ssh

To start an encrypted session with a remote networking device, use the **ssh** command in privileged EXEC or user EXEC mode.

ssh [**-v** {**1** | **2**}] [**-c** {**3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc**}] [**-l** *userid* | **-l** *userid***:***vrfname number ip-address* | **-l** *userid***:rotary***number ip-address*] [**-m** {**hmac-md5** | **hmac-md5-96** | **hmac-sha1** | **hmac-sha1-96**}] [**-o numberofpasswordprompts** *n*] [**-p** *port-num*] {*ip-addr* | *hostname*} [*command*] [**-vrf**]

Syntax Description

-v	(Optional) Specifies the version of Secure Shell (SSH) to use to connect to the server. • **1**—Connects using SSH Version 1. • ***2***—Connects using SSH Version 2.
-c {**3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc**}	(Optional) Specifies the crypto algorithms Data Encryption Standard (DES), Triple DES (3DES), or Advanced Encryption Standard (AES) to use for encrypting data. AES algorithms supported are aes128-cbc, aes192-cbc, and aes256-cbc. • To use SSH Version 1, you must have an encryption image running on the router. Cisco software images that include encryption have the designators “k8” (DES) or “k9” (3DES). • SSH Version 2 supports only the following crypto algorithms: aes128-cbc, aes192-cbc, aes256-cbc, and 3des-cbc. SSH Version 2 is supported only in 3DES images. • If you do not specify the **-c** keyword, during negotiation the remote networking device sends all the supported crypto algorithms. • If you configure the **-c** keyword and the server does not support the argument that you have shown (des, 3des, aes128-cbc, aes192-cbc, or aes256-cbc), the remote networking device closes the connection.
-l *userid*	(Optional) Specifies the user ID to use when logging in on the remote networking device running the SSH server. If no user ID is specified, the default is the current user ID.

-l *userid***:***vrfname number ip-address*	(Optional) Specifies the user ID when configuring reverse SSH by including port information in the *userid* field. • **:**—Signifies that a port number and terminal IP address will follow the user ID. • *vrfname* — User specific VRF. • *number*—Terminal or auxiliary line number. • *ip-address*—IP address of the terminal server. **Note** The *userid* argument and **:***number ip-address* delimiter and arguments must be used if you are configuring reverse SSH by including port information in the *userid* field (a method that is easier than the longer method of listing each terminal or auxiliary line on a separate command configuration line).The *vrfname* allows SSH to establish sessions with hosts whose addresses are in a VRF instance.
-l *userid***:rotary***number ip-address*	(Optional) Specifies that the terminal lines are to be grouped under the rotary group for reverse SSH. • **:**—Signifies that a rotary group number and terminal IP address will follow. • *number*—Terminal or auxiliary line number. • *ip-address*—IP address of the terminal server. **Note** The *userid* argument and **:rotary**{*number*} {*ip-address*} delimiter and arguments must be used if you are configuring reverse SSH by including rotary information in the *userid* field (a process that is easier than the longer process of listing each terminal or auxiliary line on a separate command configuration line).
-m {**hmac-md5 | hmac-md5-96 | hmac-sha1 | hmac-sha1-96**}	(Optional) Specifies a Hashed Message Authentication Code (HMAC) algorithm. • SSH Version 1 does not support HMACs. • If you do not specify the **-m** keyword, the remote device sends all the supported HMAC algorithms during negotiation. If you specify the **-m** keyword and the server does not support the argument that you have shown (hmac-md5, hmac-md5-96, hmac-sha1, and hmac-sha1-96), the remote device closes the connection.
-o numberofpasswordprompts *n*	(Optional) Specifies the number of password prompts that the software generates before ending the session. The SSH server may also apply a limit to the number of attempts. If the limit set by the server is less than the value specified by the **-o numberofpasswordprompts** keyword, the limit set by the server takes precedence. The default is 3 attempts, which is also the Cisco IOS SSH server default. The range of values is from 1 to 5.
-p *port-num*	(Optional) Indicates the desired port number for the remote host. The default port number is 22.

ip-addr | *hostname*	Specifies the IPv4 or IPv6 address or host name of the remote networking device.
command	(Optional) Specifies the Cisco IOS command that you want to run on the remote networking device. If the remote host is not running Cisco IOS software, this may be any command recognized by the remote host. If the command includes spaces, you must enclose the command in quotation marks.
-vrf	(Optional) Adds VRF awareness to SSH client side functionality. VRF instance name in the client is provided with the IP address to lookup the correct routing table and establish a connection.

Command Default

No encrypted session exists if the command is not used.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(8)T	Support for IPv6 addresses was added.
12.0(21)ST	IPv6 address support was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	IPv6 address support was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	IPv6 address support was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX	This command was integrated into Cisco IOS Release 12.2(17a)SX.
12.3(7)T	This command was expanded to include Secure Shell Version 2 support. The **-c** keyword was expanded to include support for the following cryptic algorithms: aes128-cbc, aes192-cbc, and aes256-cbc. The **-m** keyword was added, with the following algorithms: hmac-md5, hmac-md5-96, hmac-sha1, and hmac-sha1-96. The **-v** keyword and arguments **1** and **2** were added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	The **-l** *userid***:***number ip-address* and **-l** *userid***:rotary***number ip-address* keyword and argument options were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.3(7)JA	This command was integrated into Cisco IOS Release 12.3(7)JA.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	The**-l** *userid***:***vrfname number ip-address* keyword and argument and **-vrf** keyword were added.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

The **ssh** command enables a Cisco router to make a secure, encrypted connection to another Cisco router or device running an SSH Version 1 or Version 2 server. This connection provides functionality that is similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for a secure communication over an insecure network.

Note

- SSH Version 1 is supported on DES (56-bit) and 3DES (168-bit) data encryption software images only. In DES software images, DES is the only encryption algorithm available. In 3DES software images, both DES and 3DES encryption algorithms are available.
- SSH Version 2 supports only the following crypto algorithms: aes128-cbc, aes192-cbc, and aes256-cbc. SSH Version 2 is supported only in 3DES images.
- SSH Version 1 does not support HMAC algorithms.

The following example illustrates the initiation of a secure session between the local router and the remote host HQhost to run the **show users** command. The result of the **show users** command is a list of valid users who are logged in to HQhost. The remote host will prompt for the adminHQ password to authenticate the user adminHQ. If the authentication step is successful, the remote host will return the result of the **show users** command to the local router and will then close the session.

```
ssh -l adminHQ HQhost "show users"
```

The following example illustrates the initiation of a secure session between the local router and the edge router HQedge to run the **show ip route** command. In this example, the edge router prompts for the adminHQ password to authenticate the user. If the authentication step is successful, the edge router will return the result of the **show ip route** command to the local router.

```
ssh -l adminHQ HQedge "show ip route"
```

The following example shows the SSH client using 3DES to initiate a secure remote command connection with the HQedge router. The SSH server running on HQedge authenticates the session for the admin7 user on the HQedge router using standard authentication methods. The HQedge router must have SSH enabled for authentication to work.

```
ssh -l admin7 -c 3des -o numberofpasswordprompts 5 HQedge
```

The following example shows a secure session between the local router and a remote IPv6 router with the address 3ffe:1111:2222:1044::72 to run the **show running-config** command. In this example, the remote IPv6 router prompts for the adminHQ password to authenticate the user. If the authentication step is successful, the remote IPv6 router will return the result of the **show running-config** command to the local router and will then close the session.

```
ssh -l adminHQ 3ffe:1111:2222:1044::72 "show running-config"
```

Note A hostname that maps to the IPv6 address 3ffe:1111:2222:1044::72 could have been used in the last example.

The following example shows a SSH Version 2 session using the crypto algorithm aes256-cbc and an HMAC of hmac-sha1-96. The user ID is user2, and the IP address is 10.76.82.24.

```
ssh -v 2 -c aes256-cbc -m hmac-sha1-96 -1 user2 10.76.82.24
```

The following example shows that reverse SSH has been configured on the SSH client:

```
ssh -l lab:1 router.example.com
```

The following command shows that Reverse SSH will connect to the first free line in the rotary group:

```
ssh -l lab:rotary1 router.example.com
```

Related Commands

Command	Description
ip ssh	Configures SSH server control parameters on the router.
show ip ssh	Displays the version and configuration data for SSH.
show ssh	Displays the status of SSH server connections.

ssid (local RADIUS server group)

To assign up to 20 service set identifiers (SSIDs) to a user group, use the **ssid** command in local RADIUS server group configuration mode. To instruct the access point (AP) to not check if the client has come in on a list of specified SSIDs, use the **no** form of this command.

ssid *ssid-number*

no ssid *ssid-number*

Syntax Description

ssid-number	SSID number of user group members.

Defaults

No default behavior or values

Command Modes

Local RADIUS server group configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

You can enter up to 20 SSIDs to limit users to those SSIDs.

Examples

The following example shows that the SSID “green” has been added to the local user group:

```
ssid green
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.

Command	Description
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

ssl encryption

To specify the encryption algorithm that the Secure Sockets Layer (SSL) protocol uses for SSL Virtual Private Network (SSL VPN) connections, use the **ssl encryption** command in webvpn gateway configuration mode. To remove an algorithm from the SSL VPN gateway, use the **no** form of this command.

ssl encryption [**3des-sha1**] [**aes-sha1**] [**rc4-md5**]

no ssl encryption

Syntax Description

3des-sha1	(Optional) Configures the 3 DES-SHA1 encryption algorithm.
aes-sha1	(Optional) Configures the AES-SHA1 encryption algorithm.
rc4-md5	(Optional) Configures the RC4-MD5 encryption algorithm.

Defaults

All algorithms are available in the order shown above.

Command Modes

Webvpn gateway configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The SSL VPN provides remote-access connectivity from almost any Internet-enabled location using only a Web browser and its native SSL encryption. Configuring this command allows you to restrict the encryption algorithms that SSL uses in Cisco IOS software. The ordering of the algorithms specifies the preference. If you specify this command after you have specified an algorithm, the previous setting is overridden.

Examples

The following example configures the gateway to use, in order, the 3DES-SHA1, AES-SHA1, or RC4-MD5 encryption algorithms for SSL connections:

```
Router(config)# webvpn gateway SSL_GATEWAY
Router(config-webvpn-gateway)# ssl encryption rc4-md5
Router(config-webvpn-gateway)#
```

Related Commands

Command	Description
webvpn gateway	Defines a SSL VPN gateway and enters webvpn gateway configuration mode.

ssl-proxy module allowed-vlan

To add the VLANs allowed over the trunk to the Secure Socket Layer (SSL) Services Module, enter the **ssl-proxy module allowed-vlan** command in global configuration mode. To remove the SSL Services Module from the specified VLAN, use the **no** form of this command.

ssl-proxy module *mod* **allowed-vlan** *vlan-id*

no ssl-proxy module *mod* **allowed-vlan** *vlan-id*

Syntax Description

mod	Module number.
vlan-id	VLAN number; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Wireless LAN Services Module (WLSM) only.

One of the allowed VLANs must be the administrative VLAN.

To verify the configuration, enter the **show spanning-tree vlan** command.

To display the spanning-tree state for the specified VLAN, enter the **show ssl-proxy module state** command.

Examples

This example shows how to add an SSL Services Module installed in slot 6 to a specific VLAN:

```
Router (config)# ssl-proxy module 6 allowed-vlan 100
Router (config)#
```

This example shows how to remove the SSL Services Module from the specified VLAN:

```
Router (config)# no ssl-proxy module 6 allowed-vlan 100
Router (config)#
```

Related Commands

Command	Description
show ssl-proxy module state	Displays the spanning-tree state for the specified VLAN.

ssl truspoint

To configure the certificate trustpoint on a SSL VPN gateway, use the **ssl trustpoint** command in webvpn gateway configuration mode. To remove the trustpoint association, use the **no** form of this command.

ssl trustpoint *name*

no ssl trustpoint

Syntax Description

name	Name of the trust point.

Defaults

This command has no default behavior or values.

Command Modes

SSLVPN gateway configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

You can configure a persistent self-signed certificate or an external CA server to generate a valid trustpoint.

Examples

The following example configures a trustpoint named CA_CERT:

```
Router(config)# webvpn gateway SSL_GATEWAY
Router(config-webvpn-gateway)# ssl trustpoint CA_CERT
```

Related Commands

Command	Description
webvpn gateway	Defines a SSL VPN gateway and enters webvpn gateway configuration mode.

sso-server

To create a Single SignOn (SSO) server name under a Secure Sockets Layer Virtual Private Network (SSL VPN) context and to enter webvpn sso server configuration mode—and to attach an SSO server to a policy group—use the **sso-server** command in webvpn sso server configuration and group policy configuration modes, respectively. To remove an SSO server name, use the **no** form of this command.

sso-server *name*

no sso-server *name*

Syntax Description

name	Name of the SSO server.

Command Default

A SSO server is not created or attached to a policy group.

Command Modes

Webvpn sso server configuration
Group policy configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

The SSO server name is configured under the SSL VPN context in webvpn context configuration mode. All SSO server-related parameters, such as web agent URL and policy server secret key, are configured under the SSO server name. The SSO server name is attached to the policy group in webvpn group policy configuration mode.

Examples

The following example shows that the SSO server “test-sso-server” is created under the SSL VPN context and attached to a policy group named “ONE”:

```
webvpn context context1
 sso-server “test-sso-server”
  web-agent-url “http://webagent.example.com”
  secret-key “12345”
  retries 3
  timeout 15
 policy group ONE
  sso-server “test-sso-server”
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

status

To enter the signature-definition-status configuration mode, which allows you to change the enabled or retired status of an individual signature, use the **status** command in signature-definition-action configuration mode. To return to the default action, use the **no** form of this command.

status

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Signature-definition-action configuration (config-sigdef-action)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Before issuing the **status** command, you must specify at least one signature via the **signature** command.

Examples

The following example shows how to change the status of signature 9000:0 to enabled:

```
Router(config)# ip ips signature-definition
Router(config-sigdef-sig)# signature 9000 0
Router(config-sigdef-action)# status
Router(config-sigdef-status)# enabled true
```

Related Commands

Command	Description
signature	Specifies a signature for which the CLI user tunings will be changed.

strict-http

To allow HTTP messages to pass through the firewall or to reset the TCP connection when HTTP noncompliant traffic is detected, use the **strict-http** command in appfw-policy-http configuration mode. To disable configured settings, use the **no** form of this command.

strict-http action {**reset** | **allow**} [**alarm**]

no strict-http action {**reset** | **allow**} [**alarm**]

Syntax Description

action	HTTP messages are subject to the specified action (**reset** or **allow**).
reset	Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection.
allow	Forwards the packet through the firewall.
alarm	(Optional) Generates system logging (syslog) messages for the given action.

Defaults

If this command is not enabled, all traffic will be allowed through the firewall.

Command Modes

appfw-policy-http configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

The following example shows how to define the HTTP application firewall policy “mypolicy.” This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule “firewall,” which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
```

```
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

subject-alt-name

To specify the trustpoint certificate name in the Subject Alternative Name (subjectAltName) field in the X.509 certificate, which is contained in the trustpoint certificate, use the **subject-alt-name** in ca-trustpoint configuration mode. To remove this configuration, use the **no** form of this command.

subject-alt-name *name*

no subject-alt-name *name*

Syntax Description

name	Specifies the trustpoint certificate name.

Command Default

The Subject Alternative Name field is not included in the X.509 certificate.

Command Modes

Ca-trustpoint (ca-trustpoint)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

The **subject-alt-name** command is used to create a self-signed trustpoint certificate for the router that contains the trustpoint name in the Subject Alternative Name (subjectAltName) field. This Subject Alternative Name can be used only when the trustpoint enrollment option is specified for self-signed enrollment in the trustpoint policy.

Note The Subject Alternative Name field in the X.509 certificate is defined in RFC 2511.

Examples

The following example shows how to create a self-signed trustpoint certificate for the router that contains the trustpoint name in the Subject Alternative Name (subjectAltName) field:

```
Router> enable
Router# configure terminal
Router(config)# crypto pki trustpoint TESTCA
Router(ca-trustpoint)# enrollment selfsigned
Router(ca-trustpoint)# subject-alt-name TESTCA
Router(ca-trustpoint)# exit
Router(config)# cypto pki enroll TESTCA
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]:
Generate Self Signed Router Certificate? [yes/no]: yes

Router Self Signed Certificate successfully created
Router(config)# exit
```

The following certificate is created:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: CN=TESTCA/unstructuredName=r1.cisco.com
        Validity
            Not Before: Mar 22 20:26:20 2010 GMT
            Not After : Jan  1 00:00:00 2020 GMT
        Subject: CN=TESTCA/unstructuredName=r1.cisco.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (512 bit)
                Modulus (512 bit):
                    00:8d:71:2e:3b:eb:a2:e2:f3:44:d9:bc:a9:85:88:
                    f4:a9:bd:c9:7f:f0:69:f5:e7:75:8f:00:f2:8e:3e:
                    2f:ca:5e:c5:08:43:95:8c:a2:6a:ae:ce:a0:ae:82:
                    61:61:ff:4e:8c:8f:89:d1:56:d8:35:34:b7:95:93:
                    1a:72:03:71:fb
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
            CA:TRUE
            X509v3 Subject Alternative Name:
            DNS:TESTCA
            X509v3 Authority Key Identifier:
            keyid:F9:A4:95:87:5F:A4:CA:7D:65:FA:BE:38:20:55:18:F9:4C:6C:D5:F3

            X509v3 Subject Key Identifier:
            F9:A4:95:87:5F:A4:CA:7D:65:FA:BE:38:20:55:18:F9:4C:6C:D5:F3
    Signature Algorithm: md5WithRSAEncryption
        6d:92:e7:a8:a5:1a:5a:ef:13:58:02:1b:79:17:93:41:37:c9:
        2d:9f:1a:a3:f5:3a:73:05:cd:d1:02:84:43:7e:e0:84:07:46:
        55:f9:45:59:51:ba:25:48:6f:d8:e1:0d:35:44:07:5c:16:17:
        35:45:99:e2:80:6e:53:e5:35:76
-----BEGIN CERTIFICATE-----
MIIBszCCAV2gAwIBAgIBAjANBgkqhkiG9w0BAQQFADAuMQ8wDQYDVQQDEwZURVNU
Q0ExGzAZBgkqhkiG9w0BCQIWDHIxLmNpc2NvLmNvbTAeFw0xMDAzMjIyMDI2MjBa
Fw0yMDAxMDEwMDAwMDBaMC4xDzANBgNVBAMTBlRFU1RDQTEbMBkGCSqGSIb3DQEJ
AhYMcjEuY2lzY28uY29tMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAI1xLjvrouLz
RNm8qYWI9Km9yX/wafXndY8A8o4+L8pexQhDlYyiaq7OoK6CYWH/ToyPidFW2DU0
t5WTGnIDcfsCAwEAAaNmMGQwDwYDVR0TAQH/BAUwAwEB/zARBgNVHREECjAIggZU
RVNUQ0EwHwYDVR0jBBgwFoAU+aSVh1+kyn1l+r44IFUY+Uxs1fMwHQYDVR0OBBYE
FPmklYdfpMp9Zfq+OCBVGPlMbNXzMA0GCSqGSIb3DQEBBAUAA0EAbZLnqKUaWu8T
WAIbeReTQTfJLZ8ao/U6cwXN0QKEQ37ghAdGVflFWVG6JUhv2OENNUQHXBYXNUWZ
4oBuU+U1dg==
-----END CERTIFICATE-----
```

Related Commands

Command	Description
cypto pki enroll	Requests the certificates for the router from the trustpoint.
crypto pki trustpoint	Creates a trustpoint and enters ca-trustpoint configuration mode.
enrollment selfsigned	Specifies self-signed enrollment for a trustpoint.

subject-name

To specify the subject name in the certificate request, use the **subject-name** command in ca-trustpoint configuration mode. To clear any subject name from the configuration, use the **no** form of this command.

subject-name [*x.500-name*]

no subject-name [*x.500-name*]

Syntax Description

x.500-name	(Optional) Specifies the subject name used in the certificate request.

Defaults

If the *x-500-name* argument is not specified, the fully qualified domain name (FQDN), which is the default subject name, will be used.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

Before you can issue the **subject-name** command, you must enable the **crypto ca trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.

The **subject-name** command is an attribute that can be set for autoenrollment; thus, issuing this command prevents you from being prompted for a subject name during enrollment.

Examples

The following example shows how to specify the subject name for the “frog” certificate:

```
crypto ca trustpoint frog
 enrollment url http://frog.phoobin.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet-0
 auto-enroll regenerate
 password revokme
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

subnet-acl (IKEv2)

To configure split tunneling, use the **subnet-acl** command in IKEv2 authorization policy configuration mode. To remove this command from your configuration and restore the default value, use the **no** form of this command.

subnet-acl {*acl-number* | *acl-name*}

no subnet-acl

Syntax Description

acl-number	Access list number. The range is 100 to 199.
acl-name	Access list name.

Command Default

Split tunneling is disabled.

Command Modes

IKEv2 authorization policy configuration (config-ikev2-author-policy)

Command History

Release	Modification
15.1(3)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use the **subnet-acl** command to specify that the groups of ACLs represent protected subnets for split tunneling. Split tunneling is the ability to have a secure tunnel to the central site and simultaneous clear text tunnels to the Internet.

You must enable the **crypto ikev2 authorization policy** command, which specifies local group policy group authorization parameters that have to be defined or changed, before enabling the **subnet-acl** command.

Examples

The following example shows how to apply split tunneling for the group name “cisco.” In this example, all traffic sourced from the client and destined to the subnet 192.168.1.0 will be sent through the VPN tunnel.

```
crypto ikev2 authorization policy cisco
 key cisco
 dns 10.2.2.2 10.3.2.3
 pool dog
 subnet-acl 199
!
access-list 199 permit ip 192.168.1.0 0.0.0.255 any
```

Related Commands

Command	Description
crypto ikev2 authorization policy	Specifies an IKEv2 authorization policy group.

subscriber access pppoe unique-key circuit-id

To specify a unique circuit ID tag for a PPP over Ethernet (PPPoE) user session to be tapped on the router, use the **subscriber access pppoe unique-key circuit-id** command in global configuration mode. To restore the default value, use the **no** form of this command.

subscriber access pppoe unique-key circuit-id

no subscriber access pppoe unique-key circuit-id

Syntax Description

This command has no arguments or keywords.

Defaults

A unique circuit ID tag for PPPoE user session is not specified.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

In Cisco IOS XE Release 2.6, a user session is tapped based on the unique PPPoE circuit ID tag. This circuit ID tag serves as a unique parameter for the PPPoE user session on the device. The tapped user session is provisioned through SNMP, and user session data packets and RADIUS authentication data packets are tapped. This command is used in conjunction with the Lawful Intercept feature.

Related Commands

Command	Description
show idmgr session key	Verifies the user session information in the ID Manager (IDMGR) database by specifying the unique circuit ID tag using the **circuit-id** keyword and *circuit-id* argument.

subscriber service

To enable per-subscriber services, use the **subscriber service** command in global configuration mode. To disable per-subscriber services, use the **no** form of this command.

subscriber service {**accounting interim-interval** *minutes* | **coa-rfc-compliant** | **ignore** | **multiple-accept** | **password** | **police** | **session-accounting** | **shaper** | **target-atm-vc** | **vc-ignore-cos**}

no subscriber service {**accounting interim-interval** *minutes* | **coa-rfc-compliant** | **ignore** | **multiple-accept** | **password** | **police** | **session-accounting** | **shaper** | **target-atm-vc** | **vc-ignore-cos**}

Syntax Description

accounting interim-interval *minutes*	Enables the generation of interim service accounting records at periodic intervals for subscribers. The *minutes* argument indicates the number of periodic intervals to send accounting update records from 1 to 71582 minutes.
coa-rfc-compliant	Sends RFC 3576 compliant change of authorization (CoA) NAK messages.
ignore	Ignores any of per-subscriber services.
multiple-accept	Allows multiple services on access-accept.
password	Password to use when downloading services.
police	Quality of service (QoS) RADIUS service police command.
session-accounting	Enables the inclusion of activated services in a session accounting start message.
shaper	QoS RADIUS service shaper command.
target-atm-vc	Enables the QoS service on the target ATM virtual circuit (VC).
vc-ignore-cos	Ignores the set Layer 2 class of service (set-cos) value on the target ATM VC.

Command Default

Service accounting is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Release 12.2(31)ZV1	This command was introduced for session accounting and was implemented on the Cisco 10000 series router for the PRE3.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.

Usage Guidelines

The **subscriber service session-accounting** command enables the router to include all activated services in a single accounting Session-Start message for a session.

RADIUS can activate a service using the RADIUS Access-Accept message. When RADIUS activates a service on the router after the router sends the accounting Session-Start message, the router generates an accounting session update that includes all activated services.

When a session stops, all currently active services are included in the accounting session stop record.

The **subscriber service accounting interim-interval** command enables the router to generate interim service accounting records at periodic intervals for subscribers. RADIUS Attribute 85 in the user service profile always takes precedence over the configured interim-interval value. RADIUS Attribute 85 must be in the user service profile. See the RADIUS Attributes Overview and RADIUS IETF Attributes feature document for more information.

Note If RADIUS Attribute 85 is not in the user service profile, then the interim-interval value is used for service interim accounting records. The interim-interval value is configured by either using the **aaa accounting update** command in global configuration mode or the **action-type** command in accounting method list configuration mode. See the Configuring Accounting feature document for more information.

Examples

The following example enables per-service accounting:

```
Router(config)# subscriber service session-accounting
```

Related Commands

Command	Description
bandwidth account	Enables class-based fair queuing and ATM overhead accounting.
shape account	Shapes traffic to the indicated bit rate and enables ATM overhead accounting.

svc address-pool

To configure a pool of IP addresses to assign to end users in a policy group, use the **svc address-pool** command in webvpn group policy configuration mode. To remove the address pool from the policy group configuration, use the **no** form of this command.

svc address-pool *name* [**netmask** *ip-netmask*]

no svc address-pool

Syntax Description

name	Name of the address pool that is configured using the **ip local pool** command.
netmask	(Optional) Applies the IP netmask for the address pool.
ip-netmask	(Optional) IP netmask for the address pool.

Command Default

IP address pools are not assigned to end users.

Command Modes

Webvpn group policy configuration (config-webvpn-group)

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.1(1)T	This command was modified. The **netmask** keyword and *ip-netmask* argument were added.

Usage Guidelines

Before configuring the **svc address-pool** command, use the **ip local pool** command to define the address pool. The standard configuration assumes that the IP addresses in the pool are reachable from a directly connected network.

Configuring Address Pools for Networks That Are Not Directly Connected

If you need to configure an address pool for IP addresses from a network that is not directly connected, perform the following steps:

1. Create a local loopback interface and configure it with an IP address and subnet mask from the address pool.
2. Configure the address pool with the **ip local pool** command. The range of addresses must fall under the subnet mask configured in Step 1.
3. Configure the **svc address-pool** command with the name configured in Step 2.

See the "Examples" section for an example of how to configure a pool of IP addresses to assign to end users in a policy group.

Note Switched Virtual Circuits (SVC) software, or the Secure Sockets Layer Virtual Private Network (SSL VPN) client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

Directly Connected Network Example

The following example shows how to configure the 192.168.1/24 network as an address pool:

```
Router(config)# ip local pool ADDRESSES 192.168.1.1 192.168.1.254
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc address-pool ADDRESSES
Router(config-webvpn-group)# end
```

Nondirectly Connected Network Example

The following example shows how to configure the 172.16.1/24 network as an address pool. Because the network is not directly connected, a local loopback is configured.

```
Router(config)# interface loopback 0
Router(config-int)# ip address 172.16.1.128 255.255.255.0
Router(config-int)# no shutdown
Router(config-int)# exit
Router(config)# ip local pool ADDRESSES 172.16.1.1 172.16.1.254
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc address-pool ADDRESSES
```

Related Commands

Command	Description
ip local pool	Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc default-domain

To configure the Cisco AnyConnect VPN Client domain for a policy group, use the **svc default-domain** command in webvpn group policy configuration mode. To remove the domain from the policy group configuration, use the **no** form of this command.

svc default-domain *name*

no svc default-domain

Syntax Description

name	Name of the domain.

Command Default

Cisco AnyConnect VPN Client domain is not configured.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Note SVC software, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example configures cisco.com as the default domain:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc default-domain cisco.com
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc dns-server

To configure Domain Name System (DNS) servers for policy group end users, use the **svc dns-server** command in webvpn group policy configuration mode. To remove a DNS server from the policy group configuration, use the **no** form of this command.

svc dns-server {**primary** | **secondary**} *ip-address*

no svc dns-server {**primary** | **secondary**}

Syntax Description

primary | **secondary**	Configures the primary or secondary DNS server.
ip-address	An IPv4 address is entered to identify the server.

Command Default

DNS servers are not configured.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Note SVC software, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example configures primary and secondary DNS servers for the policy group:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc dns-server primary 192.168.3.1
Router(config-webvpn-group)# svc dns-server secondary 192.168.4.1
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc dpd-interval

To configure the dead peer detection (DPD) timer value for the gateway or client, use the **svc dpd-interval** command in webvpn group policy configuration mode. To remove a DPD timer value from the policy group configuration, use the **no** form of this command.

svc dpd-interval {**client** | **gateway**} *seconds*

no svc dpd-interval {**client** | **gateway**}

Syntax Description

client | **gateway**	Specifies the client or gateway.
seconds	Sets the time interval, in seconds, for the DPD timer. A number from 0 through 3600 is entered.

Command Default

The DPD timer is reset every time a packet is received over the Secure Sockets Layer Virtual Private Network (SSL VPN) tunnel from the gateway or end user.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Note SVC software, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example sets the DPD timer to 30 seconds for a SSL VPN gateway and to 5 minutes for end users (remote PC or device):

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc dpd-interval gateway 30
Router(config-webvpn-group)# svc dpd-interval client 300
Router(config-webvpn-group)#
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc dtls

To enable Datagram Transport Layer Security (DTLS) support on the Cisco IOS Secure Socket Layer Virtual Private Network (SSL VPN), use the **svc dtls** command in WebVPN group policy configuration mode. To disable the configuration, use the **no** form of this command.

svc dtls

no svc dtls

Syntax Description

This command has no arguments or keywords.

Command Default

DTLS is enabled by default on the Cisco ISR G2 series routers (3900, 2900, 1900, 890, and 880) and is disabled on other routers.

Command Modes

WebVPN group policy configuration (config-webvpn-group)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The DTLS Support for IOS SSL VPN feature enables DTLS as a transport protocol for the traffic tunneled through SSL VPN. The DTLS Support for IOS SSL VPN feature is enabled by default on the Cisco IOS SSL VPN. You can use the **no svc dtls** command to disable DTLS support on the SSL VPN.

Examples

The following example shows how to disable DTLS support on the Cisco IOS SSL VPN gateway:

```
Router# configure terminal
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group group1
Router(config-webvpn-group)# no svc dtls
```

Related Commands

Command	Description
dtls port	Configures a DTLS port.

svc homepage

To configure the URL of the web page that is displayed upon successful user login, use the **svc homepage** command in webvpn group policy configuration mode. To remove the URL from the policy group configuration, use the **no** form of this command.

svc homepage *string*

no svc homepage

Syntax Description

string	The *string* argument is entered as an HTTP URL. The URL can be up to 255 characters in length.

Command Default

URL of the home page is not configured.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Note SVC software, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example configures www.cisco.com as the Cisco AnyConnect VPN Client home page:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc homepage www.cisco.com
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc keepalive

To specify the Secure Socket Layer Virtual Private Network Client (SVC) keepalive value, use the **svc keepalive** command in webvpn group policy configuration mode. To return the **svc keepalive** command to its default, use the **no** form of this command.

svc keepalive *seconds*

no svc keepalive

Syntax Description

seconds	Specifies an SVC keepalive value from 0 to 600 seconds.

Command Default

The SVC is enabled to send keepalive messages by default with a frequency of 30 seconds.

Command Modes

Webvpn group policy configuration (config-webvpn-group)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

You can adjust the frequency of keepalive messages to ensure that an SVC connection through a proxy, IOS firewall, or Network Address Translation (NAT) device remains active, even if the device limits the time that the connection can be idle. Adjusting the frequency also ensures that the SVC does not disconnect and reconnect when the remote user is not actively running a socket-based application, such as Microsoft Outlook or Microsoft Internet Explorer.

If the **svc keepalive** command is configured with a value of **0** seconds, then the keepalive function is disabled.

Note SVC is the predecessor of Cisco AnyConnect VPN Client software.

Examples

In the following example, the security appliance is configured to enable the SVC to send keepalive messages with a frequency of 300 seconds (5 minutes), for the existing group-policy group “ONE”:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc keepalive 300
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc keep-client-installed

To configure the end user to keep Cisco AnyConnect VPN Client software installed when the SSL VPN connection is not enabled, use the **svc keep-client-installed** command in webvpn group policy configuration mode. To remove the software installation requirement from the policy group configuration, use the **no** form of this command.

svc keep-client-installed

no svc keep-client-installed

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The configuration of this command removes the overhead of pushing the Cisco AnyConnect VPN Client software to the end user on each connection attempt.

Note SVC, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example configures end users to keep Cisco AnyConnect VPN Client software installed:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc keep-client-installed
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc module

To configure Start Before Logon (SBL) functionality support for a Cisco IOS Secure Sockets Layer Virtual Private Network (SSL VPN) headend, use the **svc module** command in webvpn group policy configuration mode. To disable the configuration, use the **no** form of this command.

svc module *module-name*

no svc module

Syntax Description

module-name	Anyconnect module name.

Command Default

The SBL functionality is disabled by default.

Command Modes

Webvpn group policy configuration (config-webvpn-group)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

The SBL functionality connects the client PC to the enterprise network even before the users log in to the PC. This functionality allows the administrator to run the logon scripts even if the user is not connected to the enterprise network.

Use the **svc module** command to configure the SBL functionality support for the Cisco IOS SSL VPN headend. This command sets the module in the WebVPN cookie for the AnyConnect client, and thereby helps in downloading the SBL components to the client from the SSL VPN headend.

Examples

The following example shows how to configure the vpn1 AnyConnect module to Cisco IOS SSL VPN headend:

```
Router# configure terminal
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group group1
Router(config-webvpn-group)# svc module vpn1
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.

svc msie-proxy

To configure Microsoft Internet Explorer (MSIE) browser proxy settings for policy group end users, use the **svc msie-proxy** command in webvpn group policy configuration mode. To remove a MSIE proxy setting from the policy group configuration, use the **no** form of this command.

svc msie-proxy {**server** *host* | **exception** *host* | **option** {**auto** | **bypass-local** | **none**}}

no svc msie-proxy {**server** *host* | **exception** *host* | **option** {**auto** | **bypass-local** | **none**}}

Syntax Description

server *host*	Specifies a MSIE proxy server for policy group end users. The *host* argument specifies the location of the MSIE server. The *host* argument is configured as an IPv4 address or fully qualified domain name, followed by a colon and port number.
exception *host*	Configures the browser not to send traffic for a single Domain Name System (DNS) hostname or IP address through the proxy.
option auto	Configures the browser to automatically detect proxy settings.
option bypass-local	Configures the browser to bypass proxy settings that are configured on the remote user.
option none	Configures the browser to use no proxy settings.

Command Default

MSIE browser proxy settings are not configured for policy group end users.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The configuration of this command is applied to end users that use a MSIE browser. The configuration of this command has no effect on any other browser type.

Note SVC, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example configures automatic detection of MSIE proxy settings and configures proxy exceptions for traffic from www.example.com and the 10.20.20.1 host:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc msie-proxy option auto
Router(config-webvpn-group)# svc msie-proxy exception www.example.com
Router(config-webvpn-group)# svc msie-proxy exception 10.20.20.1
```

The following example configures a connection to an MSIE proxy server through a fully qualified domain name (FQDN) and a port number:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc msie-proxy server www.example.com:80
```

The following example configures a connection to an MSIE proxy server through an IP address and port number:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc msie-proxy server 10.10.10.1:80
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc msie-proxy server

To specify a Microsoft Internet Explorer (MSIE) proxy server for policy group end users, use the **svc msie-proxy server** command in SSLVPN group policy configuration mode. To remove the proxy server from the policy group configuration, use the **no** form of this command.

svc msie-proxy server *host*

no svc msie-proxy server

Syntax Description

host	Specifies the location of the MSIE server. The host argument is configured as an IPv4 address or fully qualified domain name, followed by a colon and port number.

Command Default

No default behavior or values.

Command Modes

SSLVPN group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following example configures a connection to an MSIE proxy server through a fully qualified domain name and a port number:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc msie-proxy server www.cisco.com:80
Router(config-webvpn-group)#
```

The following example configures a connection to an MSIE proxy server through an IP address and port number:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc msie-proxy server 10.10.10.1:80
Router(config-webvpn-group)#
```

Related Commands

Command	Description
policy group	Enters SSLVPN group policy configuration mode to configure a group policy.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

svc mtu

To configure the MTU size for a policy group at the client end, use the **svc mtu** command in webvpn group policy configuration mode. To set the MTU size to its default, use the **no** form of this command.

svc mtu *size*

no svc mtu

Syntax Description

size	Size of MTU, in bytes. Range: 256 to 1406. Default:1406

Command Default

The default MTU size is 1406.

Command Modes

Webvpn group policy configuration (config-webvpn-group)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The maximum size of prefragmented packets that is supported by the adapter is only 1406 bytes. Sending packets larger than 1406 bytes could cause potential problems; as a result, there is a size restriction.

Examples

The following example configures the MTU size to 778 bytes:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc mtu 778
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure an SSL VPN context.

svc rekey

To configure the time and method that a tunnel key is refreshed for policy group end users, use the **svc rekey** command in webvpn group policy configuration mode. To remove the tunnel key configuration from the policy group configuration, use the **no** form of this command.

svc rekey {**method** {**new-tunnel** | **ssl**} | **time** *seconds*}

no svc rekey {**method** {**new-tunnel** | **ssl**} | **time** *seconds*}

Syntax Description

method new-tunnel	Refreshes the tunnel key by creating a new tunnel connection to the end user.
method ssl	Refreshes the tunnel key by renegotiating the Secure Sockets Layer (SSL) session.
time *seconds*	Configures the time interval, in seconds, at which the tunnel key is refreshed. A number from 0 through 43200 seconds is entered.

Command Default

Time and method are not configured.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Note SVC, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example configures the tunnel key to be refreshed by initiating a new tunnel connection once an hour:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc rekey method new-tunnel
Router(config-webvpn-group)# svc rekey time 3600
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn configuration mode to configure the SSL VPN context.

svc split

To enable split tunneling for Cisco AnyConnect VPN Client tunnel clients, use the **svc split** command in webvpn group policy configuration mode. To remove the split tunneling configuration from the policy group configuration, use the **no** form of this command.

svc split {**include** | **exclude** [**local-lans**]} {*ip-address mask* | **acl** {*access-list-number* | *access-list-name*}}

no svc split {**include** | **exclude** [**local-lans**]} {*ip-address mask* | **acl**}

Syntax Description

include	Specifies the traffic to be sent over Secure Sockets Layer Virtual Private Network (SSL VPN) tunnel. Traffic from the specified IP address and mask is resolved through the Cisco AnyConnect VPN Client tunnel.
exclude	Specifies the traffic not to be sent over SSL VPN tunnel. Traffic from the specified IP address and mask is not resolved through the Cisco AnyConnect VPN Client tunnel.
local-lans	Specifies the traffic for local LANs not to be sent over SSL VPN tunnel.
ip-address mask	Destination network prefix.
acl	Specifies access-list identifier for classifying the tunnel traffic.
access-list-number	Standard IP access-list number. Range is from 1 to 99.
access-list-name	Access-list name.

Command Default

Split tunneling is not enabled for Cisco AnyConnect VPN Client tunnel clients.

Command Modes

WebVPN group policy configuration (config-webvpn-group)

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.1(1)T	This command was modified. The **acl** keyword and the *access-list* and *access-list-name* arguments were added.

Usage Guidelines

Split tunnel support allows you to configure a policy that permits specific traffic to be carried outside the Cisco AnyConnect VPN Client tunnel. Traffic is either included (resolved in tunnel) or excluded (resolved through the Internet service provider [ISP] or WAN connection). Tunnel resolution configuration is mutually exclusive. An IP address cannot be both included and excluded at the same time. Entering the **local-lans** keyword permits the remote user to access resources on a local LAN, such as a network printer.

Note Switched Virtual Circuits (SVC), or the Secure Sockets Layer Virtual Private Network (SSL VPN) client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example shows how to configure a list of IP addresses to be resolved over the tunnel (included) and a list to be resolved outside of the tunnel (excluded):

```
Router(config-webvpn-group)# svc split exclude 192.168.1.0 255.255.255.0
Router(config-webvpn-group)# svc split include 172.16.1.0 255.255.255.0
```

Related Commands

Command	Description
policy group	Enters WebVPN group policy configuration mode to configure a policy group.
webvpn context	Enters WebVPN configuration mode to configure the SSL VPN context.

svc split dns

To configure the Secure Sockets Layers Virtual Private Network (SSL VPN) gateway to resolve the specified fully qualified Domain Name System (DNS) names through the Cisco AnyConnect VPN Client tunnel, use the **svc split dns** command in webvpn group policy configuration mode. To remove the split DNS statement from the policy group configuration, use the **no** form of this command.

svc split dns *name*

no svc split dns *name*

Syntax Description

dns *name*	The *name* argument is entered as a fully qualified DNS name.

Command Default

The SSL VPN gateway is not configured to resolve the specified fully qualified DNS names through the Cisco AnyConnect VPN Client tunnel.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Entering this command configures the SSL VPN gateway to resolve the specified DNS suffixes (domains) through the tunnel. The gateway automatically incudes the default domain into the list of domains that are resolved through the tunnel. Up to 10 DNS statements can be configured.

Note SVC, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example configures primary and secondary DNS servers for the policy group:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc split dns cisco.com
Router(config-webvpn-group)# svc split dns my.company.net
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc wins-server

To configure Windows Internet Name Service (WINS) servers for policy group end users, use the **svc wins-server** command in webvpn group policy configuration mode. To remove a WINS server from the policy group configuration, use the **no** form of this command.

svc wins-server {**primary** | **secondary**} *ip-address*

no svc dns-server {**primary** | **secondary**}

Syntax Description

primary | **secondary**	Configures the primary or secondary WINS server.
ip-address	An IPv4 address is entered to identify the server.

Command Default

WINS servers are not configured for policy group end users.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Note SVC, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example configures primary and secondary WINS servers for the policy group:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc wins-server primary 172.31.1.1
Router(config-webvpn-group)# svc wins-server secondary 172.31.2.1
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

switchport port-security

To enable port security on an interface, use the **switchport port-security** command in interface configuration mode. To disable port security, use the **no** form of this command.

switchport port-security

no switchport port-security

Syntax Description

This command has no keywords or arguments.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720: • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Follow these guidelines when configuring port security:

- With Release 12.2(18)SXE and later releases, port security is supported on trunks.
- With releases earlier than Release 12.2(18)SXE, port security is not supported on trunks.
- With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports.
- With releases earlier than Release 12.2(18)SXE, port security is not supported on 802.1Q tunnel ports.
- A secure port cannot be a destination port for a Switch Port Analyzer (SPAN).
- A secure port cannot belong to an EtherChannel.
- A secure port cannot be a trunk port.
- A secure port cannot be an 802.1X port. If you try to enable 802.1X on a secure port, an error message appears, and 802.1X is not enabled. If you try to change an 802.1X-enabled port to a secure port, an error message appears, and the security settings are not changed.

Examples

This example shows how to enable port security:

```
Router(config-if)# switchport port-security
```

This example shows how to disable port security:

Related Commands

Command	Description
show port-security	Displays information about the port-security setting.

switchport port-security aging

To configure the port security aging, use the **switchport port-security aging time** command in interface configuration mode. To disable aging, use the **no** form of this command.

switchport port-security aging {**time** *time* | **type** {**absolute** | **inactivity**}}

no switchport port-security aging

Syntax Description

time *time*	Sets the duration for which all addresses are secured; valid values are from 1 to 1440 minutes.
type	Specifies the type of aging.
absolute	Specifies absolute aging; see the "Usage Guidelines" section for more information.
inactivity	Specifies that the timer starts to run only when there is no traffic; see the "Usage Guidelines" section for more information.

Defaults

The defaults are as follows:

- Disabled.
- If enabled, the defaults are as follows:
  - *time* is 0.
  - **type** is **absolute**.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720: • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports. • The **type**, **absolute**, and **inactivity** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Follow these guidelines when configuring port security:

- With Release 12.2(18)SXE and later releases, port security is supported on trunks. With releases earlier than Release 12.2(18)SXE, port security is not supported on trunks.
- With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports. With releases earlier than Release 12.2(18)SXE, port security is not supported on 802.1Q tunnel ports.

You can apply one of two ty**p**es of aging for automatically learned addresses on a secure port:

- Absolute aging times out the MAC address after the age-time has been exceeded, regardless of the traffic pattern. This default is for any secured port, and the age-time is set to 0.
- Inactivity aging times out the MAC address only after the age_time of inactivity from the corresponding host has been exceeded.

Examples

This example shows how to set the aging time as 2 hours:

```
Router(config-if)# switchport port-security aging time 120
```

This example shows how to set the aging time as 2 minutes:

```
Router(config-if)# switchport port-security aging time 2
```

This example shows how to set the aging type on a port to absolute aging:

```
Router(config-if) switchport port-security aging type absolute
```

This example shows how to set the aging type on a port to inactivity aging:

```
Router(config-if) switchport port-security aging type inactivity
```

Related Commands

Command	Description
show port-security	Displays information about the port-security setting.

switchport port-security mac-address

To add a MAC address to the list of secure MAC addresses, use the **switchport port-security mac-address** command. To remove a MAC address from the list of secure MAC addresses, use the **no** form of this command.

switchport port-security mac-address {*mac-addr* | {**sticky** [*mac-addr*]} [**vlan** *vlan* | *vlan-list*]}

no switchport port-security mac-address {*mac-addr* | {**sticky** [*mac-addr*]} [**vlan** *vlan* | *vlan-list*]}

Syntax Description

mac-addr	MAC addresses for the interface; valid values are from 1 to 1024.
sticky	Configures the dynamic MAC addresses as sticky on an interface.
vlan *vlan* | *vlan-list*	(Optional) Specifies a VLAN or range of VLANs; see the "Usage Guidelines" section for additional information.

Defaults

This command has no default settings.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720: • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports. • The **vlan** *vlan* | *vlan-list* keyword and arguments were added. • The **sticky** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you configure fewer secure MAC addresses than the maximum number of secure MAC addresses on all interfaces, the remaining MAC addresses are dynamically learned.

To clear multiple MAC addresses, you must enter the **no** form of this command once for each MAC address to be cleared.

The *vlan-list* argument is visible only if the port has been configured and is operational as a trunk. Enter the **switchport mode trunk** command and then enter the **switchport nonegotiate** command.

The **sticky** keyword configures the dynamic MAC addresses as sticky on an interface. Sticky MAC addresses configure the static Layer 2 entry to stay sticky to a particular interface. This feature can prevent MAC moves or prevent the entry from being learned on a different interface.

You can configure the sticky feature even when the port security feature is not enabled on the interface. It becomes operational once port security is enabled on the interface.

Note You can enter the **switchport port-security mac-address sticky** command only if sticky is enabled on the interface.

When port security is enabled, disabling the sticky feature causes all configured and learned sticky addresses to be deleted from the configuration and converted into dynamic secure addresses.

When port security is disabled, disabling the sticky feature causes all configured and learned sticky addresses to be deleted from the configuration.

Examples

This example shows how to configure a secure MAC address:

```
Router(config-if)# switchport port-security mac-address 1000.2000.3000
```

This example shows how to delete a secure MAC address from the address table:

```
Router(config-if)# no switchport port-security mac-address 1000.2000.3000
```

This example shows how to enable the sticky feature on an interface:

```
Router(config-if)# switchport port-security mac-address sticky
```

This example shows how to disable the sticky feature on an interface:

```
Router(config-if)# no switchport port-security mac-address sticky
```

This example shows how to make a specific MAC address as a sticky address:

```
Router(config-if)# switchport port-security mac-address sticky 0000.0000.0001
```

This example shows how to delete a specific sticky address:

```
Router(config-if)# no switchport port-security mac-address sticky 0000.0000.0001
```

This example shows how to delete all sticky and static addresses that are configured on an interface:

```
Router(config-if)# no switchport port-security mac-address
```

Related Commands

Command	Description
clear port-security	Deletes configured secure MAC addresses and sticky MAC addresses from the MAC address table.
show port-security	Displays information about the port-security setting.
switchport mode trunk	Configures the port as a trunk member.
switchport nonegotiate	Configures the LAN port into permanent trunking mode.

switchport port-security maximum

To set the maximum number of secure MAC addresses on a port, use the **switchport port-security maximum** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

switchport port-security maximum *maximum* [**vlan** *vlan* | *vlan-list*]

no switchport port-security maximum

Syntax Description

maximum	Maximum number of secure MAC addresses for the interface; valid values are from 1 to 4097.
vlan *vlan* | *vlan-list*	(Optional) Specifies a VLAN or range of VLANs; see the "Usage Guidelines" section for additional information.

Defaults

This command has no default setings.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720 only: • The maximum number of secure MAC addresses was changed from 1024 to 4097. • The **vlan** *vlan* | *vlan-list* keyword and arguments were added. • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you enter this command more than once, subsequent use of this command overrides the previous value of *maximum*. If the new *maximum* argument is larger than the current number of the secured addresses on this port, there is no effect except to increase the value of the *maximum*.

If the new *maximum* is smaller than the old *maximum* and there are more secure addresses on the old *maximum*, the command is rejected.

If you configure fewer secure MAC addresses than the maximum number of secure MAC addresses on the port, the remaining MAC addresses are dynamically learned.

Once the maximum number of secure MAC addresses for the port is reached, no more addresses are learned on that port even if the per-VLAN port maximum is different from the aggregate maximum number.

You can override the maximum number of secure MAC addresses for the port for a specific VLAN or VLANs by entering the **switchport port-security maximum** *maximum* **vlan** *vlan* | *vlan-list* command.

The *vlan-list* argument allows you to enter ranges, commas, and delimited entries such as 1,7,9-15,17.

The *vlan-list* argument is visible only if the port has been configured and is operational as a trunk. Enter the **switchport mode trunk** command and then enter the **switchport nonegotiate** command.

Examples

This example shows how to set the maximum number of secure MAC addresses that are allowed on this port:

```
Router(config-if)# switchport port-security maximum 5
```

This command shows how to override the maximum set for a specific VLAN:

```
Router(config-if)# switchport port-security maximum 3 vlan 102
```

Related Commands

Command	Description
show port-security	Display information about the port-security setting.
switchport nonegotiate	Configures the LAN port into permanent trunking mode.

switchport port-security violation

To set the action to be taken when a security violation is detected, use the **switchport port-security violation** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

switchport port-security violation{**shutdown** | **restrict** | **protect**}

no switchport port-security violation{**shutdown** | **restrict** | **protect**}

Syntax Description

shutdown	Shuts down the port if there is a security violation.
restrict	Drops all the packets from the insecure hosts at the port-security process level and increments the security-violation count.
protect	Drops all the packets from the insecure hosts at the port-security process level but does not increment the security-violation count.

Command Default

The port security violation is shutdown.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720: • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(14)SXH	**Platform port-security disable traps** was introduced as part of protect violation mode.

Usage Guidelines

When a security violation is detected, one of the following actions occurs:

- Protect—When the number of port-secure MAC addresses reaches the maximum limit that is allowed on the port, the packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses.

  Platform port-security disable traps is configurable only when the violation mode is set to **protect**. When this option is configured, drop entries will not be installed into hardware for violating

addresses, thus allowing traffic to continue to flow to violating address from legitimate ports. To protect switch CPU against overload when this option is enabled, we recommend that you configure the port-security rate-limiter to 2000 packets per second with a burst rate of 10.

Note This feature also permits traffic to legitimate ports from insecure MAC addresses.

- Restrict—A port-security violation restricts data and causes the security-violation counter to increment.
- Shutdown—The interface is error disabled when a security violation occurs.

Note When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause psecure-violation** global configuration command or you can manually reenable it by entering the **shutdown** and **no shutdown** commands in interface-configuration mode.

Examples

This example shows how to set the action to be taken when a security violation is detected:

```
Router(config-if)# switchport port-security violation restrict
```

This example allows the traffic to a secured MAC address on one port to flow even in the presence of violations on other ports while in protect mode.

```
Router(config-if)# switchport port-security violation protect
Router(config-if)# platform port-security disable traps
```

Related Commands

Command	Description
show port-security	Displays information about the port-security setting.
errdisable recovery cause psecure-violation (global configuration)	Removes a secure port from an error-disabled state.
platform port-security disable traps	Modifies the behavior of protect violation mode.

tacacs-server administration

To enable the handling of administrative messages by the TACACS+ daemon, use the **tacacs-server administration** command in global configuration mode. To disable the handling of administrative messages by the TACACS+ daemon, use the **no** form of this command.

tacacs-server administration

no tacacs-server administration

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Prior to 12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows that the TACACS+ daemon is enabled to handle administrative messages:

```
tacacs-server administration
```

tacacs-server directed-request

To send only a username to a specified server when a direct request is issued, use the **tacacs-server directed-request** command in global configuration mode. To send the entire string to the TACACS+ server, use the **no** form of this command.

tacacs-server directed-request [**restricted**] [**no-truncate**]

no tacacs-server directed-request

Syntax Description

restricted	(Optional) Restrict queries to directed request servers only.
no-truncate	(Optional) Do not truncate the @hostname from the username.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command sends only the portion of the username before the "@" symbol to the host specified after the "@" symbol. In other words, with the directed-request feature enabled, you can direct a request to any of the configured servers, and only the username is sent to the specified server.

Disabling **tacacs-server directed-request** causes the whole string, both before and after the "@" symbol, to be sent to the default TACACS+ server. When the directed-request feature is disabled, the router queries the list of servers, starting with the first one in the list, sending the whole string, and accepting the first response that it gets from the server. The **tacacs-server directed-request** command is useful for sites that have developed their own TACACS+ server software that parses the whole string and makes decisions based on it.

With **tacacs-server directed-request** enabled, only configured TACACS+ servers can be specified by the user after the "@" symbol. If the host name specified by the user does not match the IP address of a TACACS+ server configured by the administrator, the user input is rejected.

Use **no tacacs-server directed-request** to disable the ability of the user to choose between configured TACACS+ servers and to cause the entire string to be passed to the default server.

Examples

The following example disables **tacacs-server directed-request** so that the entire user input is passed to the default TACACS+ server:

```
no tacacs-server directed-request
```

tacacs-server dns-alias-lookup

To enable IP Domain Name System (DNS) alias lookup for TACACS+ servers, use the command in global configuration mode. To disable IP DNS alias lookup, use the **no** form of this command.

tacacs-server dns-alias-lookup

no tacacs-server dns-alias-lookup

Syntax Description

This command has no arguments or keywords.

Command Default

IP DNS alias lookup is disabled.

Command Modes

global configuration

Command History

Release	Modification
Prior to 12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows that IP DNS alias lookup has been enabled:

```
tacacs-server dns-alias-lookup
```

tacacs-server domain-stripping

To configure a network access server (NAS) to strip suffixes, or to strip both suffixes and prefixes from the username before forwarding the username to the remote TACACS+ server, use the **tacacs-server domain-stripping** command in global configuration mode. To disable a stripping configuration, use the **no** form of this command.

tacacs-server domain-stripping [[**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] | **strip-suffix** *suffix*] [**vrf** *vrf-name*]

no tacacs-server domain-stripping [[**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] | **strip-suffix** *suffix*] [**vrf** *vrf-name*]

Syntax Description

right-to-left	(Optional) Specifies that the NAS will apply the stripping configuration at the first delimiter found when parsing the full username from right to left. The default is for the NAS to apply the stripping configuration at the first delimiter found when parsing the full username from left to right.
prefix-delimiter *character* [*character2...character7*]	(Optional) Enables prefix stripping and specifies the character or characters that will be recognized as a prefix delimiter. Valid values for the *character* argument are @, /, $, %, \, #, and -. Multiple characters can be entered without intervening spaces. Up to seven characters can be defined as prefix delimiters, which is the maximum number of valid characters. If a \ is entered as the final or only value for the *character* argument, it must be entered as \\. No prefix delimiter is defined by default.
delimiter *character* [*character2...character7*]	(Optional) Specifies the character or characters that will be recognized as a suffix delimiter. Valid values for the *character* argument are @, /, $, %, \, #, and -. Multiple characters can be entered without intervening spaces. Up to seven characters can be defined as suffix delimiters, which is the maximum number of valid characters. If a \ is entered as the final or only value for the *character* argument, it must be entered as \\. The default suffix delimiter is the @ character.
strip-suffix *suffix*	(Optional) Specifies a suffix to strip from the username.
vrf *vrf-name*	(Optional) Restricts the domain stripping configuration to a Virtual Private Network (VPN) routing and forwarding (VRF) instance. The *vrf-name* argument specifies the name of a VRF.

Command Default

Stripping is disabled. The full username is sent to the TACACS+ server.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
XE 2.5	This command was integrated into Cisco IOS Release XE 2.5.

Usage Guidelines

Use the **tacacs-server domain-stripping** command to configure the NAS to strip the domain from a username before forwarding the username to the TACACS+ server. If the full username is user1@cisco.com, enabling the **tacacs-server domain-stripping** command results in the username "user1" being forwarded to the TACACS+ server.

Use the **right-to-left** keyword to specify that the username should be parsed for a delimiter from right to left, rather than from left to right. This allows strings with two instances of a delimiter to strip the username at either delimiter. For example, if the username is user@cisco.com@cisco.net, the suffix could be stripped in two ways. The default direction (left to right) would result in the username "user" being forwarded to the TACACS+ server. Configuring the **right-to-left** keyword would result in the username "user@cisco.com" being forwarded to the TACACS+ server.

Use the **prefix-delimiter** keyword to enable prefix stripping and to specify the character or characters that will be recognized as a prefix delimiter. The first configured character that is parsed will be used as the prefix delimiter, and any characters before that delimiter will be stripped.

Use the **delimiter** keyword to specify the character or characters that will be recognized as a suffix delimiter. The first configured character that is parsed will be used as the suffix delimiter, and any characters after that delimiter will be stripped.

Use **strip-suffix** *suffix* to specify a particular suffix to strip from usernames. For example, configuring the **tacacs-server domain-stripping strip-suffix cisco.net** command would result in the username user@cisco.net being stripped, while the username user@cisco.com will not be stripped. You may configure multiple suffixes for stripping by issuing multiple instances of the **tacacs-server domain-stripping** command. The default suffix delimiter is the @ character.

Note Issuing the **tacacs-server domain-stripping strip-suffix** *suffix* command disables the capacity to strip suffixes from all domains. Both the suffix delimiter and the suffix must match for the suffix to be stripped from the full username. The default suffix delimiter of @ will be used if you do not specify a different suffix delimiter or set of suffix delimiters using the **delimiter** keyword.

Note Issuing the **no tacacs-server host command** enables you to reconfigure the tacacs-server host information. You can view the contents of the current running configuration file using the **show running-config** command.

To apply a domain-stripping configuration only to a specified VRF, use the **vrf** *vrf-name* option.

The interactions between the different types of domain stripping configurations are as follows:

- You may configure only one instance of the **tacacs-server domain-stripping** [**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] command.
- You may configure multiple instances of the **tacacs-server domain-stripping** [**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] [**vrf** *vrf-name*] command with unique values for **vrf** *vrf-name*.

- You may configure multiple instances of the **tacacs-server domain-stripping strip-suffix** *suffix* [**vrf** *per-vrf*] command to specify multiple suffixes to be stripped as part of a global or per-VRF ruleset.
- Issuing any version of the **tacacs-server domain-stripping** command automatically enables suffix stripping using the default delimiter character @ for that ruleset, unless a different delimiter or set of delimiters is specified.
- Configuring a per-suffix stripping rule disables generic suffix stripping for that ruleset. Only suffixes that match the configured suffix or suffixes will be stripped from usernames.

Examples

The following example configures the router to parse the username from right to left and sets the valid suffix delimiter characters as @, \, and $. If the full username is cisco/user@cisco.com$cisco.net, the username “cisco/user@cisco.com” will be forwarded to the TACACS+ server because the $ character is the first valid delimiter encountered by the NAS when parsing the username from right to left.

```
tacacs-server domain-stripping right-to-left delimiter @\$
```

The following example configures the router to strip the domain name from usernames only for users associated with the VRF instance named abc. The default suffix delimiter @ will be used for generic suffix stripping.

```
tacacs-server domain-stripping vrf abc
```

The following example enables prefix stripping using the character / as the prefix delimiter. The default suffix delimiter character @ will be used for generic suffix stripping. If the full username is cisco/user@cisco.com, the username “user” will be forwarded to the TACACS+ server.

```
tacacs-server domain-stripping prefix-delimiter /
```

The following example enables prefix stripping, specifies the character / as the prefix delimiter, and specifies the character # as the suffix delimiter. If the full username is cisco/user@cisco.com#cisco.net, the username “user@cisco.com” will be forwarded to the TACACS+ server.

```
tacacs-server domain-stripping prefix-delimiter / delimiter #
```

The following example enables prefix stripping, configures the character / as the prefix delimiter, configures the characters $, @, and # as suffix delimiters, and configures per-suffix stripping of the suffix cisco.com. If the full username is cisco/user@cisco.com, the username “user” will be forwarded to the TACACS+ server. If the full username is cisco/user@cisco.com#cisco.com, the username “user@cisco.com” will be forwarded.

```
tacacs-server domain-stripping prefix-delimiter / delimiter $@#
tacacs-server domain-stripping strip-suffix cisco.com
```

The following example configures the router to parse the username from right to left and enables suffix stripping for usernames with the suffix cisco.com. If the full username is cisco/user@cisco.net@cisco.com, the username “cisco/user@cisco.net” will be forwarded to the TACACS+ server. If the full username is cisco/user@cisco.com@cisco.net, the full username will be forwarded.

```
tacacs-server domain-stripping right-to-left
tacacs-server domain-stripping strip-suffix cisco.com
```

The following example configures a set of global stripping rules that will strip the suffix cisco.com using the delimiter @, and a different set of stripping rules for usernames associated with the VRF named myvrf:

```
tacacs-server domain-stripping strip-suffix cisco.com
```

```
!
tacacs-server domain-stripping prefix-delimiter # vrf myvrf
tacacs-server domain-stripping strip-suffix cisco.net vrf myvrf
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
ip vrf	Defines a VRF instance and enters VRF configuration mode.
radius-server domain-stripping	Configures a router to strip a prefix or suffix from the username before forwarding the username to the RADIUS server.

tacacs-server host

To specify a TACACS+ host, use the **tacacs-server host** command in global configuration mode. To delete the specified name or address, use the **no** form of this command.

tacacs-server host {*host-name* | *host-ip-address*} [**key** *string*] [**nat**] [**port** [*integer*]] [**single-connection**] [**timeout** [*integer*]]

no tacacs-server host {*host-name* | *host-ip-address*}

Syntax Description

host-name	Name of the host.
host-ip-address	IP address of the host.
key	(Optional) Specifies an authentication and encryption key. This must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the global command **tacacs-server key** for this server only.
string	(Optional) Character string specifying authentication and encryption key.
nat	(Optional) Port Network Address Translation (NAT) address of the client is sent to the TACACS+ server.
port	(Optional) Specifies a TACACS+ server port number. This option overrides the default, which is port 49.
integer	(Optional) Port number of the server. Valid port numbers range from 1 through 65535.
single-connection	(Optional) Maintains a single open connection between the router and the TACACS+ server.
timeout	(Optional) Specifies a timeout value. This overrides the global timeout value set with the **tacacs-server timeout** command for this server only.
integer	(Optional) Integer value, in seconds, of the timeout interval. The value is from 1 through 1000.

Defaults

No TACACS+ host is specified.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1(11), 12.2(6)	The **nat** keyword was added.
12.2(8)T	The **nat** keyword was integrated into Cisco IOS Release 12.2(8)T.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can use multiple **tacacs-server host** commands to specify additional hosts. The Cisco IOS software searches for hosts in the order in which you specify them. Use the **port**, **timeout**, **key,** **single-connection**, and **nat** keywords only when running a AAA/TACACS+ server.

Because some of the parameters of the **tacacs-server host** command override global settings made by the **tacacs-server timeout** and **tacacs-server key** commands, you can use this command to enhance security on your network by uniquely configuring individual routers.

The **single-connection** keyword specifies a single connection (only valid with CiscoSecure Release 1.0.1 or later). Rather than have the router open and close a TCP connection to the server each time it must communicate, the single-connection option maintains a single open connection between the router and the server. The single connection is more efficient because it allows the server to handle a higher number of TACACS operations.

Examples

The following example specifies a TACACS+ host named Sea_Change:

```
tacacs-server host Sea_Change
```

The following example specifies that, for authentication, authorization, and accounting (AAA) confirmation, the router consults the TACACS+ server host named Sea_Cure on port number 51. The timeout value for requests on this connection is three seconds; the encryption key is a_secret.

```
tacacs-server host Sea_Cure port 51 timeout 3 key a_secret
```

Related Commands

Command	Description
aaa authentication	Specifies or enables AAA authentication.
aaa authorization	Sets parameters that restrict user access to a network.
aaa accounting	Enables AAA accounting of requested services for billing or security.
ppp	Starts an asynchronous connection using PPP.
slip	Starts a serial connection to a remote host using SLIP.
tacacs-server key	Sets the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon.

tacacs-server key

To set the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon, use the **tacacs-server key** command in global configuration mode. To disable the key, use the **no** form of this command.

tacacs-server key {**0** *string* | **7** *string* | *string*}

no tacacs-server key {**0** *string* | **7** *string* | *string*}

Syntax Description

0 *string*	Specifies that an unencrypted key will follow. • *string*—The unencrypted (clear text) shared key.
7 *string*	Specifies that a hidden key will follow. • *string*—The hidden shared key.
string	The unencrypted (clear text) shared key.

Defaults

No default behavior or values.

Command Modes

Global configuration(#)

Command History

Release	Modification
11.1	This command was introduced.
12.3(2)T	The **0** *string* and **7** *string* keywords and argument pairs were added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2(33)SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

After enabling authentication, authorization, and accounting (AAA) with the **aaa new-model** command, you must set the authentication and encryption key using the **tacacs-server key** command.

The key entered must match the key used on the TACACS+ daemon. All leading spaces are ignored; spaces within and at the end of the key are not. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

Examples

The following example sets the authentication and encryption key to “dare to go”:

```
Router(config)#tacacs-server key dare to go
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
tacacs-server host	Specifies a TACACS+ host.

tacacs-server packet

To specify the maximum size of TACACS+ packets, use the **tacacs-server packet** command in global configuration mode. To disable, use the **no** form of this command.

tacacs-server packet maxsize *size*

no tacacs-server packet maxsize

Syntax Description

maxsize *size*	Specifies maximum TACACS+ packet size. The range is from 10240 to 65536.

Command Default

The default maximum size for a TACAC+ packet is 65536.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0	This command was introduced in a release earlier than Cisco IOS Release 12.0
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to set the the maximum TACACS+ packet size to 10240:

```
tacacs-server packet maxsize 10240
```

tacacs-server timeout

To set the interval for which the TACACS server waits for a server host to reply, use the **tacacs-server timeout** command in global configuration mode. To restore the default timeout interval, use the **no** form of this command.

tacacs-server timeout *seconds*

no tacacs-server timeout

Syntax Description

seconds	Timeout interval, in seconds. The range is from 1 to 1000. The default is 5.

Command Default

The default timeout interval for which the server waits for the server host to reply is 5 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **tacacs-server timeout** command to set the interval for which the server waits for a server host to reply. A TCP connection between the server and the host times out during higher loads. Therefore, to delay TCP timeouts, change the timeout interval to 30 seconds. You can also configure the **tacacs-server host** command with the **single-connection** keyword to delay TCP timeouts.

Examples

The following example shows how to set the timeout interval to 20 seconds:

```
Router# configure terminal
Router(config)# tacacs-server timeout 20
```

Related Commands

Command	Description
tacacs-server host	Specifies a TACACS+ host.

target-value

To define the target value rating for a host, use the **target-value** command in configuration rule configuration mode. To change the target value rating or revert to the default value, use the **no** form of this command.

target-value {**mission-critical | high | medium | low**} **target-address** *ip-address* [*/nn* | **to** *ip-address*]

no target-value {**mission-critical | high | medium | low**} **target-address** *ip-address* [*/nn* | **to** *ip-address*]

Syntax Description

mission-critical | high | medium | low	Rates how important the system is to the network.
target-address *ip-address* [*/nn* | **to** *ip-address*]	A host, which can consist of a single IP address or a range of IP addresses.

Command Default

medium

Command Modes

Configuration rule configuration (config-rul)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use the **target-value** command to set the target value rating, which allows users to develop security policies that can be more strict for some resources than others. The security policy is applied to a table of hosts that are protected by Cisco IOS Intrusion Prevention System (IPS). A host can be a single IP address or a range of IP addresses with an associated target value rating.

Note Changes to the target value rating is not shown in the run time config because the changes are recorded in the seap-delta.xml file, which can be located via the **ip ips config location** command.

Examples

The following example shows how to change the target value to low for the host 192.168.0.1:

```
configure terminal
ip ips event-action-rules
 target-value low target-address 192.168.0.1
```

tcp finwait-time

To specify how long a TCP session will be managed after the Cisco IOS firewall detects a FIN-exchange, use the **tcp finwait-time** command in parameter-map type inspect configuration mode. To disable this function, use the **no** form of this command.

tcp finwait-time *seconds*

no tcp finwait-time *seconds*

Syntax Description

seconds	Amount of time, in seconds, that a TCP session will be managed after the firewall detects a FIN-exchange. The default is 5.

Command Default

None

Command Modes

Parameter-map type inspect configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The finwait-time is the time you wait for the closing sequence during a TCP connection.

When you are configuring an inspect type parameter map, you can enter the **tcp finwait-time** subcommand after you enter the **parameter-map type inspect** command.

When the software detects a valid TCP packet that is the first in a session, the software establishes state information for the new session.

Use this command to define how long TCP session state information will be maintained after the firewall detects a FIN-exchange for the session. The FIN-exchange occurs when the TCP session is ready to close.

The global value specified for this timeout applies to all TCP sessions.

The timeout set with this command is referred to as the finwait timeout.

For more detailed information about creating a parameter map, see the **parameter-map type inspect** command.

Examples

The following example changes the finwait timeout to 5 seconds:

```
parameter-map type inspect eng_network_profile
 tcp finwait-time 5
```

Related Commands

Command	Description
ip inspect tcp finwait-time	Defines how long a TCP session will still be managed after the firewall detects a FIN-exchange.
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

tcp idle-time

To configure the timeout for TCP sessions, use the **tcp idle-time** command in parameter-map type inspect configuration mode. To disable this function, use the **no** form of this command.

tcp idle-time *seconds*

no tcp idle-time *seconds*

Syntax Description

seconds	Amount of time, in seconds, that a TCP session will still be managed while there is no activity. The default is 3600 seconds (1 hour).

Command Default

None

Command Modes

Parameter-map type inspect configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

When you are configuring an inspect type parameter map, you can enter the **tcp idle-time** subcommand after you enter the **parameter-map type inspect** command.

When the software detects a valid TCP packet that is the first in a session, the software establishes state information for the new session.

If the software detects no packets for the session for a time period defined by the TCP idle timeout, the software will not continue to manage state information for the session.

The value specified for this timeout applies to all TCP sessions.

For more detailed information about creating a parameter map, see the **parameter-map type inspect** command.

Examples

The following example sets the TCP timeout to 90 seconds:

```
parameter-map type inspect eng-network-profile
 tcp idle-time 90
```

Related Commands

Command	Description
ip inspect tcp idle-time	Specifies the TCP idle timeout (the length of time a TCP session will still be managed while there is no activity).
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

tcp max-incomplete

To specify threshold and blocking time values for TCP host-specific denial-of-service (DoS) detection and prevention, use the **tcp max-incomplete** command in parameter-map type inspect configuration mode. To reset the threshold and blocking time to the default values, use the **no** form of this command.

tcp max-incomplete host *threshold* [**block-time** *minutes*]

no tcp max-incomplete host *threshold* [**block-time** *minutes*]

Syntax Description

host *threshold*	Number of half-open TCP sessions with the same host destination address that can simultaneously exist before the software starts deleting half-open sessions to the host. The range is from 1 to 2147483647. The default is unlimited.
block-time *minutes*	(Optional) Amount of time, in minutes, the software prevents connections to the host. The default is 0.

Command Default

The thresholds is unlimited, and the blocking time value is 0.

Command Modes

Parameter-map type inspect configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

When you are configuring an inspect type parameter map, you can enter the **tcp max-incomplete** subcommand after you enter the **parameter-map type inspect** command.

After the specified threshold is exceeded, the router drops packets.

Half-open means that the session has not reached the established state.An unusually high number of half-open sessions with the same destination host address could indicate that a DoS attack is being launched against the host.

When the number of half-open sessions with the same destination host address rises above a threshold (the host threshold number), the software deletes half-open sessions according to one of the following methods.

- If the **block-time** *minutes* timeout is 0 (the default):

  The software deletes the oldest existing half-open session for the host for every new connection request to the host. This ensures that the number of half-open sessions to a given host never exceeds the threshold.

- If the **block-time** *minutes* timeout is greater than 0:

  The software deletes all existing half-open sessions for the host and then blocks all new connection requests to the host. The software continues to block all new connection requests until the block-time expires.

The software also sends syslog messages whenever the specified threshold is exceeded and when blocking of connection initiations to a host starts or ends.

The global values specified for the threshold and blocking time apply to all TCP connections that Cisco IOS stateful packet inspection inspects.

For more detailed information about creating a parameter map, see the **parameter-map type inspect** command.

Examples

The following example shows how to specifiy a maximum of 100 half-open sessions and a block time of 10 minutes. If a single host receives 400 half-open sessions, subsequent connections after 100 will be dropped. If a host receives 50 connections and another host receives 50 connections, no packets are dropped.

```
parameter-map type inspect eng-network-profile
 tcp max-incomplete host 100 block-time 10
```

Related Commands

Command	Description
ip inspect tcp max-incomplete host	Specifies threshold and blocking time values for TCP host-specific DoS detection and prevention.
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

tcp reassembly memory limit

To specify the limit of the out-of-order (OOO) queue size for TCP sessions, use the **tcp reassembly memory limit** command in parameter map type OOO global configuration mode. To disable the configuration, use the **no** form of this command.

tcp reassembly memory limit *queue-size*

no tcp reassembly memory limit

Syntax Description

queue-size	Queue size, in kilobytes (KB). The range is from 1 to 4194303.

Command Default

The default OOO queue size is 1024 KB.

Command Modes

Parameter map type OOO global configuration (config-profile)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.1(3)T	This command was modified. The maximum limit value for the *queue-size* argument was changed from 4294967295 to 4194303.

Usage Guidelines

You must use the **tcp reassembly memory limit** command to specify the limit of the OOO queue size for TCP sessions when the deep packet inspection feature is configured on the router.

Examples

The following example shows how to specify 200 KB as the OOO queue size for TCP sessions:

```
Router(config)# parameter-map type ooo global
Router(config-profile)# tcp reassembly memory limit 200
```

Related Commands

Command	Description
tcp reassembly queue length	Specifies the length of the OOO queue parameters.
tcp reassembly timeout	Specifies the timeout for the OOO TCP queues.
tcp reassembly alarm	Specifies the alert message configuration for the TCP sessions.

tcp syn-flood limit

To configure a limit to the number of TCP half-open sessions before triggering synchronization (SYN) cookie processing for new SYN packets, use the **tcp syn-flood limit** command in profile configuration mode. To disable the configuration, use the **no** form of this command.

tcp syn-flood limit *maximum-session-limit*

no tcp syn-flood limit *maximum-session-limit*

Syntax Description

maximum-session-limit	Maximum number of sessions. Valid values are from 1 to 4294967295.

Command Default

No limit to the number of TCP half-open sessions are set.

Command Modes

Profile configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Usage Guidelines

A TCP half-open session is a session that has not reached the established state.

In a VRF-aware firewall, you can configure a limit to the number of TCP half-open sessions for each VRF. At both the global level and at the VPN Routing and Forwarding (VRF) level, when the configured TCP SYN flood limit is reached, the TCP SYN cookie verifies the source of the half-open sessions before creating more sessions.

You must configure the **parameter-map type inspect-vrf** or the **parameter-map type inspect global** command before you can configure the **tcp syn-flood limit** command.

Examples

The following example shows how to limit the number of TCP half-open sessions to 500 at an inspect-VRF parameter map level:

```
Router(config)# parameter-map type inspect-vrf
Router(config-profile)# tcp syn-flood limit 500
Router(config-profile)# end
```

The following example shows how to limit the number of TCP half-open sessions to 300 at a global parameter map level:

```
Router(config)# parameter-map type global
Router(config-profile)# tcp syn-flood limit 300
Router(config-profile)# end
```

Related Commands

Command	Description
parameter-map type global	Configures a global parameter map and enters profile configuration mode.
parameter-map type inspect-vrf	Configures a parameter map of type inspect VRF and enters profile configuration mode.

tcp syn-flood rate per-destination

To configure a TCP synchronization (SYN) flood rate limit for each destination address, use the **tcp syn-flood rate per-destination** command in profile configuration mode. To disable TCP SYN flood packets, use the **no** form of this command.

tcp syn-flood rate per-destination *maximum-packet-rate*

no tcp syn-flood rate per-destination *maximum-packet-rate*

Syntax Description

maximum-packet-rate	Maximum rate of TCP SYN packets. Valid values are from 1 to 1000000000.

Command Default

No TCP SYN-flood packets are configured.

Command Modes

Profile configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Usage Guidelines

When the configured maximum packet rate is reached, the TCP SYN cookie protection is triggered.

You must configure the **parameter-map type inspect-zone** or the **parameter-map type global** command before you can configure the **tcp syn-flood rate per-destination** command.

Examples

The following example shows how to configure the TCP SYN-flood packet rate of 500 at an inspect-zone parameter map level:

```
Router(config)# parameter-map type inspect-zone
Router(config-profile)# tcp syn-flood rate per-destination 500
Router(config-profile)# end
```

The following example shows how to configure the TCP SYN-flood packet rate of 300 at a global parameter map level:

```
Router(config)# parameter-map type global
Router(config-profile)# tcp syn-flood rate per-destination 300
Router(config-profile)# end
```

Related Commands

Command	Description
parameter-map type global	Configures a global parameter map and enters profile configuration mode.
parameter-map type inspect-zone	Configures a parameter map of type inspect zone and enters profile configuration mode.

tcp synwait-time

To specify how long the software will wait for a TCP session to reach the established state before dropping the session, use the **tcp synwait-time** command in parameter-map type inspect configuration mode. To disable this function, use the **no** form of this command.

tcp synwait-time *seconds*

no tcp synwait-time *seconds*

Syntax Description

seconds	Time, in seconds, that the system will wait for a TCP session to reach the established state before dropping the session. The default is 5.

Command Default

None

Command Modes

Parameter-map type inspect configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

When you are configuring an inspect type parameter map, you can enter the **tcp synwait-time** subcommand after you enter the **parameter-map type inspect** command.

For more detailed information about creating a parameter map, see the **parameter-map type inspect** command.

Examples

The following example specifies that the TCP session will be dropped if the TCP session does not reach the established state in 3 seconds:

```
parameter-map type inspect eng-network-profile
 tcp synwait-time 3
```

Related Commands

Command	Description
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

tcp window-scale-enforcement loose

To configure Cisco IOS software to disable the window scale option check in the parameter map for a TCP packet that has an invalid window scale option under the Zone Based Firewall (ZBF), use the **tcp window-scale-enforcement loose** command in parameter map configuration mode. To return to the command default, use the **no** form of this command.

tcp window-scale-enforcement loose

no tcp window-scale-enforcement loose

Command Default

The strict window scale option check is enabled in the firewall by default.

Command Modes

Parameter map configuration (config-profile)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The window scale extension expands the definition of the TCP window to 32 bits and then uses a scale factor to carry this 32-bit value in the 16-bit Window field of the TCP header. Cisco IOS software enforces strict checking of the TCP window scale option. See section 2 of RFC1323, “TCP Window Scale Option,” for more information on this function.

There are occasions when a server may be using a non-RFC compliant TCP/IP protocol stack. In this case, the initiator does not offer the window scale option, but the responder has the option enabled with a window scale factor that is not zero.

Cisco IOS administrators who experience issues with a noncompliant server may not have control over the server to which they need to connect. Disabling the Cisco IOS firewall to connect to the noncompliant server is not desirable and may fail if each endpoint cannot agree on the window scaling factor to use for its respective receive window.

The **tcp window-scale-enforcement loose** command is used in parameter map configuration mode to allow noncompliant window scale negotiation and works without the firewall being disabled to access the noncompliant servers. This command works under ZBF, which provides unidirectional firewall policy between groups of interfaces known as zones.

An older firewall strategy used by the Cisco IOS involved the configuration of Context-based Access Control (CBAC). CBAC intelligently filters TCP and UDP packets based on application-layer protocol session information. CBAC inspects traffic that travels through the firewall to discover and manage state information for TCP and UDP sessions. CBAC is configured using an inspect rule only on interfaces. This state information is used to create temporary openings in the firewall's access lists to allow return traffic and additional data connections for permissible sessions. Traffic entering or leaving the configured interface is inspected based on the direction that the inspect rule was applied.

Examples

The following example configures the IOS to disable the window scale option check in the ZBF firewall parameter map for a TCP packet that has an invalid window scale option:

```
Router# config
Router(config)# parameter-map type inspect zone3
Router(config-profile)# tcp window-scale-enforcement loose
```

Related Commands

Command	Description
tcp synwait-time	Specifies how long the software will wait for a TCP session to reach the established state before dropping the session.

template (identity policy)

To specify a virtual template from which commands may be cloned, use the **template** command in identity policy configuration mode. To disable the virtual template, use the **no** form of this command.

template {**virtual-template** *template-number*}

no template {**virtual-template** *template-number*}

Syntax Description

virtual-template	Specifies the virtual template interface that will serve as the configuration clone source for the virtual interface that is dynamically created for authenticated users.
template-number	Template interface number. The value ranges from 1 through 200.

Defaults

A virtual template from which commands may be cloned is not specified.

Command Modes

Identity policy configuration (config-identity-policy)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

The **identity policy** command must be entered in global configuration mode before the **template** command can be used.

Examples

The following example shows that an identity policy and a template have been specified:

```
Router (config)# identity policy mypolicy
Router (config-identity-policy)# template virtual-template 1
```

Related Commands

Command	Description
identity policy	Creates an identity policy.

template (identity profile)

To specify a virtual template from which commands may be cloned, use the **template** command in identity profile configuration mode. To disable the virtual template, use the **no** form of this command.

template *virtual-template*

no template *virtual-template*

Syntax Description

virtual-template	Specifies the virtual template interface that will serve as the configuration clone source for the virtual interface that is dynamically created for authenticated users.

Defaults

A virtual template from which commands may be cloned is not specified.

Command Modes

Identity profile configuration

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

The **identity profile** command and **default** keyword must be entered in global configuration mode before the **template** command can be used.

Examples

The following example shows that a default identity profile and a template have been specified:

```
Router (config)# identity profile default
Router (config-identity-prof)# template virtualtemplate1
```

Related Commands

Command	Description
description	Enters an identity profile description.
device	Statically authorizes or rejects individual devices.
identity profile	Creates an identity profile.

template config

To specify a remote URL for a Cisco IOS command-line interface (CLI) configuration template, use the **template config** command in tti-registrar configuration mode. To remove the template from the configuration and use the default configuration template, use the **no** form of this command.

template config *url* [**post**]

no template config *url*

Syntax Description

url	One of the keywords in Table 219.
post	(Optional) Specifies that the registrar will issue an HTTP POST to the external management system. The HTTP POST will include information about the device such as the device name, the current Cisco IOS version, and the current configuration in order for the external management system to return a Cisco IOS configuration more specific to the device. **Note** Common Gateway Interface (CGI) scripts must be issued with the **post** keyword.

Defaults

A default template will be used.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(6)T	The **post** keyword was added.

Usage Guidelines

Use the **template config** command to specify a URL in which to retrieve the template that will be sent from the Secure Device Provisioning (SDP) registrar to the SDP petitioner during the Trusted Transitive Introduction (TTI) exchange.

If neither a configuration template nor the **post** keyword is specified, the default configuration template is used. The default configuration template contains the following commands:

```
!
$t
!
$c
!
! end

END_CONFIG
;
```

The variable “$t” will be expanded to include a Cisco IOS public key infrastructure (PKI) trustpoint that is configured for autoenrollment with the certificate server of the registrar. The variable “$c” will be expanded into the correct certificate chain for the certificate server of the registrar.

If an external template is specified, it must include the “$t” and “$c” variables to enable the petitioner device to obtain a certificate. The **end** command must be specified. If you want to specify details about the trustpoint, you can specify a template as follows:

```
!
crypto ca trustpoint $t
 enrollment url http://<registrar fqdn>
 rsakeypair $k $s
 auto-enroll 70
!
$c
end
```

Where $t comes from “trustpoint” configured under the petitioner, $k comes from “rsakeypair” under the trustpoint:

```
! $l will be replaced by 'mytp.'
crypto provisioning petitioner
  trustpoint mytp
! $k will be replaced by 'mykey.'
crypto ca trustpoint mytp
rsakeypair mykey
!
```

Note The template configuration location may include a variable “$n”, which is expanded to the name of the introducer.

Table 219 lists the available options for the *url* argument.

Table 219 URL Keywords for the CLI Template

Keyword	Description
cns:	Retrieves from the Cisco Networking Services (CNS) configuration engine.
flash:	Retrieves from flash memory.
ftp:	Retrieves from the FTP network server.
http:	Retrieves from a HTTP server (also called a web server).
https:	Retrieves from a Secure HTTP (HTTPS) server.
null:	Retrieves from the file system.
nvram:	Retrieves from the NVRAM of the router.
rcp:	Retrieves from a remote copy (rcp) protocol network server.
scp:	Retrieves from a network server that supports Secure Shell (SSH).
system:	Retrieves from system memory, which includes the running configuration.
tftp:	Retrieves from a TFTP network server.
webflash:	Retrieves from the file system.
xmodem:	Retrieves from a network machine that uses the Xmodem protocol.

Expanded SDP CGI Template Support

Expanded SDP CGI template support allows you to specify a bootstrap configuration based on the client type, model, Cisco IOS version, and current configuration. Specifying a boot strap configuration is accomplished by the TTI registrar forwarding the device information to the external management system when requesting a bootstrap configuration.

The **template config** command with the **post** keyword supports expanded SDP CGI templates by allowing the SDP registrar to send the additional information about the device configuration to an external management system by issuing an HTTP POST or an HTTPS POST. Without the use of the **post** keyword, the SDP registrar requests information only from the management system based on the device name.

Note In order to use the expanded SDP CGI support, the registrar must be running Cisco IOS Release 12.4(6)T or a later release, the **template config** command must be issued with the **post** keyword, and the *url* argument must include either the HTTP or HTTPS protocol. No other protocol (for example, FTP) is supported for the expanded CGI template functionality.

The additional information sent to the external management system with the issuance of an HTTP POST from the SDP registrar to the external management system is shown in Table 220.

Table 220 AV Pairs Sent During HTTP Post to External Management System

AV Pair	Description
TTIFixSubjectName	AAA_AT_TTI_SUBJECTNAME (sent only if the realm authentication user is not the root user on the registrar)
TTIIosRunningConfig	Output of **show running-config brief**
TTIKeyHash	Digest calculated over the device public key
TTIPrivilege	AAA_AT_TTI_PRIVILEGE—"admin" is sent if the user is an administrator; "user" is sent if the user is not an administrator (sent only if the realm authentication user is an administrator and the information is available from the authentication, authorization, and accounting [AAA] server)
TTISignature	Digest calculated over all attribute-value (AV) pairs except UserDeviceName and TTISignCert
TTISignCert	Device current certificate (sent only if the device currently has a certificate)
TTITemplateVar	AAA_AT_TTI_IOSCONFIG(1-9) (sent only if the realm authentication user is not the root user on the registrar)
TTIUserName	Device name as entered by the administrative introducer (sent only if the realm authentication user is an administrator)
TTIVersion	TTI version of the registrar

Examples

The following example shows how to specify the HTTP URL "http://pki1-36a.cisco.com:80" for the Cisco IOS CLI configuration template, which is sent from the SDP registrar to the external management system during the TTI exchange:

```
crypto provisioning registrar
 pki-server cs1
 template config http://pki1-36a.cisco.com:80
```

The following example shows how to specify that the SDP registrar will send additional device information to the external management system to retrieve a more specific bootstrap configuration file:

```
crypto provisioning registrar
 pki-server cs1
 template config http://myserver/cgi-bin/mycgi post
```

Related Commands

Command	Description
authentication list (tti-registrar)	Authenticates the introducer in an SDP operation.
authorization list (tti-registrar)	Specifies the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS CLI snippet that is sent back to the petitioner in an SDP operation.
template username	Establishes a template username and password to access the configuration template on the file system.

template file

To specify the source template file location on the registrar and the destination template file location on the petitioner, use the **template file** command in tti-registrar configuration mode.

template file *sourceURL destinationURL*

Syntax Description

sourceURL	Specifies the source URL on the registrar for the template file using one of the keywords in Table 220.
destinationURL	Specifies the destination URL on the petitioner for template file using one of the keywords in Table 220.

Command Default

None

Command Modes

tti-registrar configuration (tti-registrar)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Use the **template file** command to specify the location where a template file will be retrieved from and copied to during the Trusted Transitive Introduction (TTI) exchange. There may be up to nine template files transferred, each with a different source and destination location. A destination URL could also be a token on the petitioner, such as usbtoken0:.

The file content is expanded on the registrar. The destination URL and file content are expanded on the petitioner.

Table 221 Source and Destination URL Keywords

Keyword	Description
archive:	Retrieves from the archive location.
cns:	Retrieves from the Cisco Networking Services (CNS) configuration engine.
disk0:	Retrieves from disk0.
disk1:	Retrieves from disk1.
flash:	Retrieves from flash memory.
ftp:	Retrieves from the FTP network server.
http:	Retrieves from a HTTP server.
https:	Retrieves from a Secure HTTP (HTTPS) server.
null:	Retrieves from the file system.

Table 221 Source and Destination URL Keywords (continued)

Keyword	Description
nvram:	Retrieves from the NVRAM of the router.
rcp:	Retrieves from a remote copy (rcp) protocol network server.
scp:	Retrieves from a network server that supports Secure Shell (SSH).
system:	Retrieves from system memory, which includes the running configuration.
tar:	Retrieves from a compressed file in tar format.
tftp:	Retrieves from a TFTP network server.
tmpsys:	Retrieves from a temporary system location.
unix:	Retrieves from the UNIX system location.
usbtoken:	Retrieves from the USB token.

Examples

The following example shows how to specify where the source template file is located and where the template file will be copied to on the petitioner:

```
crypto provisioning registrar
  pki-server cs1
  template file http://myserver/file1 usbtoken0://file1
  template file http://myserver/file2 flash://file2
```

Related Commands

Command	Description
binary file	Specifies the binary file location on the registrar and the destination binary file location on the petitioner.
crypto provisioning registrar	Configures a device to become an SDP registrar and enter tti-registrar configuration mode.

template http admin-introduction

To use a custom administrator introduction template rather than the default template, issue the **template http admin-introduction** command in tti-registrar configuration mode.

template http admin-introduction *URL*

Syntax Description

URL	Location of the custom administrator introduction template.

Command Default

If this command is not issued, the default template will be used.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

You may want to use a custom administrator introduction template rather than a default template because the device name can be prefilled on the web page for the user. Without this command, the welcome page must be the first page requested by the user.

Examples

The following example shows how to direct the registrar to use the administrator introduction page template located at tftp://walnut.cisco.com/admin-introducer.html:

```
template http admin-introduction tftp://walnut.cisco.com/admin-introducer.html
```

Related Commands

Command	Description
template http completion	Uses a custom completion template rather than the default template.
template http error	Uses a custom error template rather than the default template.
template http introduction	Uses a custom introduction template rather than the default template.
template http start	Directs the TTI registrar to use the custom start page template.
template http welcome	Uses a custom welcome template rather than the default template.

template http completion

To use a custom completion template rather than the default template, issue the **template http completion** command in tti-registrar configuration mode.

template http completion *URL*

Syntax Description

URL	Location of the custom completion template.

Command Default

If this command is not issued, the default template will be used.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Custom templates allow for additional information specific to the deployment to be displayed on the web pages. The easy way to define a custom template is to modify the default template.

Examples

The following example shows how to direct the registrar to use the completion page template located at specified location:

```
template http completion tftp://walnut.cisco.com/completion.html
```

Related Commands

Command	Description
template http admin-introduction	Uses a custom admin-introduction template rather than the default template.
template http error	Uses a custom error template rather than the default template.
template http introduction	Uses a custom introduction template rather than the default template.
template http start	Directs the TTI registrar to use the custom start page template.
template http welcome	Uses a custom welcome template rather than the default template.

template http error

To use a custom error template rather than the default template, issue the **template http error** command in tti-registrar configuration mode.

template http error *URL*

Syntax Description

URL	Location of the custom error template.

Command Default

If this command is not issued, the default template will be used.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Custom templates allow for additional information specific to the deployment to be displayed on the web pages. The easy way to define a custom template is to modify the default template.

Examples

The following example shows how to direct the registrar to use the error page template located at specified location:

```
template http error tftp://walnut.cisco.com/error.html
```

Related Commands

Command	Description
template http admin-introduction	Uses a custom admin-introduction template rather than the default template.
template http completion	Uses a custom completion template rather than the default template.
template http introduction	Uses a custom introduction template rather than the default template.
template http start	Directs the TTI registrar to use the custom start page template.
template http welcome	Uses a custom welcome template rather than the default template.

template http introduction

To use a custom introduction template rather than the default template, issue the **template http introduction** command in tti-registrar configuration mode.

template http introduction *URL*

Syntax Description

URL	Location of the custom introduction template.

Command Default

If this command is not issued, the default template will be used.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

From a custom introduction page, the completion URL of the petitioner may be prefilled on the page for the user.

Examples

The following example shows how to direct the registrar to use the customer introduction template located at specified location:

```
template http introduction tftp://walnut.cisco.com/introduction.html
```

Related Commands

Command	Description
template http admin-introduction	Uses a custom admin-introduction template rather than the default template.
template http completion	Uses a custom completion template rather than the default template.
template http start	Directs the TTI registrar to use the custom start page template.
template http welcome	Uses a custom welcome template rather than the default template.

template http start

To direct the Trusted Transitive Introduction (TTI) registrar to use the custom start page template, issue the **template http start** command in tti-registrar configuration mode.

template http start *URL*

Syntax Description

URL	Location of the start page template.

Command Default

If this command is not issued, the welcome page will be the initial communication between the introducer and the petitioner.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Use the **template http start** command to display the start page on the registrar and make that page the starting point of the TTI transaction. From the start page, the registrar can direct the user to the welcome page on the petitioner.

Examples

The following example shows how to direct the registrar to use the start page template located at the specified location:

```
template http start tftp://walnut.cisco.com/start.html
```

Related Commands

Command	Description
template http admin-introduction	Uses a custom admin-introduction template rather than the default template.
template http completion	Uses a custom completion template rather than the default template.
template http introduction	Uses a custom introduction template rather than the default template.
template http welcome	Uses a custom welcome template rather than the default template.

template http welcome

To use a custom welcome template rather than the default template, issue the **template http welcome** command in tti-registrar configuration mode.

template http welcome *URL*

Syntax Description

URL	Location of the custom welcome template.

Command Default

If this command is not issued, the default template will be used.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

From a custom welcome page, the introduction URL of the registrar may be prefilled on the page for the user.

Examples

The following example shows how to direct the registrar to use the welcome page template located at specified location:

```
template http welcome tftp://walnut.cisco.com/welcome.html
```

Related Commands

Command	Description
template http admin-introduction	Uses a custom admin-introduction template rather than the default template.
template http completion	Uses a custom completion template rather than the default template.
template http introduction	Uses a custom introduction template rather than the default template.
template http start	Directs the TTI registrar to use the custom start page template.

template location

To specify the location of the template that the SDP Registrar should use while responding to a request received through the URL profile, use the **template location** command in tti-registrar configuration mode. To remove this configuration, use the **no** form of this command.

template location *location*

no template location *location*

Syntax Description

location	Specifies the template location for the SDP Registrar.

Command Default

No template location is associated with the SDP Registrar.

Command Modes

Tti-registrar configuration mode (tti-registrar)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **template location** command is required in the SDP registrar configuration, which is used to deploy Apple iPhones on a corporate network.

Examples

The following example configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network from global configuration mode:

```
Router(config)# crypto provisioning registrar
Router(tti-registrar)# url-profile start START
Router(tti-registrar)# url-profile intro INTRO
Router(tti-registrar)# match url /sdp/intro
Router(tti-registrar)# match authentication trustpoint apple-tp
Router(tti-registrar)# match certificate cat 10
Router(tti-registrar)# mime-type application/x-apple-aspen-config
Router(tti-registrar)# template location flash:intro.mobileconfig
Router(tti-registrar)# template variable p iphone-vpn
```

Related Commands

Command	Description
crypto provisioning registrar	Configures a device to become a registrar for the SDP exchange and enters tti-registrar configuration mode.
url-profile	Specifies a URL profile that configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network.
match authentication trustpoint	Enters the trustpoint name that should be used to authenticate the peer's certificate.

Command	Description
match certificate	Enters the name of the certificate map used to authorize the peer's certificate.
match url	Specifies the URL to be associated with the URL profile.
mime-type	Specifies the MIME type that the SDP registrar should use to respond to a request received through the URL profile.
template location	Specifies the location of the template that the SDP Registrar should use while responding to a request received through the URL profile.
template variable p	Specifies the value that goes into the OU field of the subject name in the certificate to be issued.

template username

To establish a template username in which to access the file system, use the **template username** command in tti-registrar configuration mode.

template username *name*

Syntax Description

name	Template username.

Defaults

A template username is not established.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the **template username** command to create a username-based authentication system that allows you to access the configuration template, which is sent from the Secure Device Provisioning (SDP) registrar to the SDP petitioner during the Trusted Transitive Introduction (TTI) exchange.

Examples

The following example shows how to create the username “mycs” to access the configuration template for the TTI exchange:

```
crypto wui tti registrar
 pki-server cs1
 template username mycs
```

Related Commands

Command	Description
crypto wui tti registrar	Configures a device to become an SDP registrar and enters tti-registrar configuration mode.
template config	Specifies a remote URL for a Cisco IOS CLI configuration template.

template variable p

To specify the value that goes into the Organizational Unit (OU) field of the subject name in the trustpoint certificate to be issued by the SDP Registrar, use the **template variable** command in tti-registrar configuration mode. To remove this configuration, use the **no** form of this command.

template variable p *value*

no template variable p *value*

Syntax Description

value	Specifies the OU field value.

Command Default

No OU field value is associated with the trustpoint certificate.

Command Modes

Tti-registrar configuration mode (tti-registrar)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **template variable p** command can be specified optionally in the SDP registrar configuration.

Examples

The following example configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network from global configuration mode:

```
Router(config)# crypto provisioning registrar
Router(tti-registrar)# url-profile start START
Router(tti-registrar)# url-profile intro INTRO
Router(tti-registrar)# match url /sdp/intro
Router(tti-registrar)# match authentication trustpoint apple-tp
Router(tti-registrar)# match certificate cat 10
Router(tti-registrar)# mime-type application/x-apple-aspen-config
Router(tti-registrar)# template location flash:intro.mobileconfig
Router(tti-registrar)# template variable p iphone-vpn
```

Related Commands

Command	Description
crypto provisioning registrar	Configures a device to become a registrar for the SDP exchange and enters tti-registrar configuration mode.
url-profile	Specifies a URL profile that configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network.
match authentication trustpoint	Enters the trustpoint name that should be used to authenticate the peer's certificate.
match certificate	Enters the name of the certificate map used to authorize the peer's certificate.

Command	Description
match url	Specifies the URL to be associated with the URL profile.
mime-type	Specifies the MIME type that the SDP registrar should use to respond to a request received through the URL profile.
template location	Specifies the location of the template that the SDP Registrar should use while responding to a request received through the URL profile.

test aaa group

To associate a dialed number identification service (DNIS) or calling line identification (CLID) user profile with the record that is sent to the RADIUS server or to manually test load balancing server status, use the **test aaa group** command in privileged EXEC mode.

DNIS and CLID User Profile

test aaa group {*group-name* | **radius**} *username password* **new-code** [**profile** *profile-name*]

RADIUS Server Load Balancing Manual Testing

test aaa group *group-name* [**server** *ip-address*] [**auth-port** *port-number*] [**acct-port** *port-number*] *username password* **new-code** [**count** *n*] [**rate** *m*] [**blocked** {**yes** | **no**}]

Syntax Description

group-name	Subset of RADIUS servers that are used as defined by the server group *group-name*.
radius	Uses RADIUS servers for authentication.
username	Specifies a name for the user. **Caution** If you use this command to manually test RADIUS load balancing server state, it is recommended that a test user, one that is not defined on the RADIUS server, be used to protect against security issues that may arise if the test user is not correctly configured.
password	Character string that specifies the password.
new-code	The code path through the new code, which supports a CLID or DNIS user profile association with a RADIUS server.
profile *profile-name*	(Optional) Identifies the user profile specified in the **aaa user profile** command. To associate a user profile with the RADIUS server, the user profile name must be identified.
server *ip-address*	(Optional) For RADIUS server load balancing, specifies which server in the server group the test packets will be sent to.
auth-port	(Optional) Specifies the User Datagram Protocol (UDP) destination port for authentication requests.
port-number	(Optional) Port number for authentication requests; the host is not used for authentication if set to 0. If unspecified, the port number defaults to 1646.
acct-port	(Optional) Specifies the UDP destination port for accounting requests.
port-number	(Optional) Port number for accounting requests; the host is not used for accounting if set to 0. If unspecified, the port number defaults to 1646.
count *n*	(Optional) Specifies how many authentication and accounting requests are to be sent to the server for each port. • Default is 1. • Range for *n* is 1 – 50000.

rate *m*	(Optional) Specifies how many requests per second will be sent to the server. • Default is 10 requests per second. • Range for *m* is 1 – 1000.
blocked {**yes** | **no**}	(Optional) Specifies if the request will be sent in blocking or nonblocking mode. If **blocked** keyword is not used: • Default is blocking mode if one request is sent. • Default is nonblocking mode if more than one request is sent.

Command Defaults

DNIS and CLID User Profile

If this command is not enabled, DNIS or CLID attribute values will not be sent to the RADIUS server.

RADIUS Server Load Balancing Manual Testing

RADIUS server load balancing server status manual testing will not occur.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(28)SB	The following keywords and arguments were added for configuring RADIUS load balancing manual testing functionality: **server** *ip-address*, **auth-port** *port-number*, **acct-port** *port-number*, **count** *n*, **rate** *m*, **blocked**.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The **test aaa group** command can be used to

- Associate a DNIS or CLID named user profile with the record that is sent to the RADIUS server, which can then access DNIS or CLID information when the server receives a RADIUS record.
- Verify RADIUS load balancing server status.

Note The **test aaa group** command does not work with TACACS+.

Examples

The following example shows how to configure a dnis = dnisvalue user profile named “prfl1” and associate it with a **test aaa group** command:

```
aaa user profile prfl1
  aaa attribute dnis
  aaa attribute dnis dnisvalue
  no aaa attribute clid
! Attribute not found.
```

```
  aaa attribute clid clidvalue
  no aaa attribute clid
  exit
!
! Associate the dnis user profile with the test aaa group command.
test aaa group radius user1 pass new-code profile prfl1
```

The following example shows the response from a load-balanced RADIUS server that is alive when the username "test" does not match a user profile. The server is verified alive when it issues an Access-Reject response to a AAA packet generated by the **test aaa group** command.

```
Router# test aaa group SG1 test lab new-code

00:06:07: RADIUS/ENCODE(00000000):Orig. component type = INVALID
00:06:07: RADIUS/ENCODE(00000000): dropping service type, "radius-server attribute 6
on-for-login-auth" is off
00:06:07: RADIUS(00000000): Config NAS IP: 192.0.2.4
00:06:07: RADIUS(00000000): sending
00:06:07: RADIUS/ENCODE: Best Local IP-Address 192.0.2.141 for Radius-Server 192.0.2.176
00:06:07: RADIUS(00000000): Send Access-Request to 192.0.2.176:1645 id 1645/1, len 50
00:06:07: RADIUS:  authenticator CA DB F4 9B 7B 66 C8 A9 - D1 99 4E 8E A4 46 99 B4
00:06:07: RADIUS:  User-Password       [2]   18  *
00:06:07: RADIUS:  User-Name           [1]   6   "test"
00:06:07: RADIUS:  NAS-IP-Address      [4]   6   192.0.2.141
00:06:07: RADIUS: Received from id 1645/1 192.0.2.176:1645, Access-Reject, len 44
00:06:07: RADIUS:  authenticator 2F 69 84 3E F0 4E F1 62 - AB B8 75 5B 38 82 49 C3
00:06:07: RADIUS:  Reply-Message       [18]  24
00:06:07: RADIUS:   41 75 74 68 65 6E 74 69 63 61 74 69 6F 6E 20 66  [Authentication ]
00:06:07: RADIUS:   61 69 6C 75 72 65                               [failure]
00:06:07: RADIUS(00000000): Received from id 1645/1
00:06:07: RADIUS/DECODE: Reply-Message fragments, 22, total 22 bytes
```

Related Commands

Command	Description
aaa attribute	Adds DNIS or CLID attribute values to a user profile.
aaa user profile	Creates a AAA user profile.
load-balance	Enables RADIUS server load balancing for RADIUS-named server groups.
radius-server host	Enables RADIUS automated testing for load balancing.
radius-server load-balance	Enables RADIUS server load balancing for the global RADIUS server group.

test crypto self-test

To test the crypto configuration to see if it passes or fails, use the **test crypto self-test** command in privileged or user EXEC mode.

test crypto self-test

Syntax Description

This command has no arguments or keywords.

Command Default

Privileged EXEC (#)

User EXEC (>)

Command History

Release	Modification
12.2XN	This command was introduced.

Usage Guidelines

As a result of the test, a new SELF_TEST_RESULT system log is generated. If the crypto test fails, a SELF_TEST_FAILURE system log is generated.

Examples

The following example displays the output of the **test crypto self-test** command:

```
Router# test crypto self-test
*Apr 23 01:48:49.678: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Self test ac)
*Apr 23 01:48:49.822: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (DH self test)
*Apr 23 01:48:49.954: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Software Cry)
*Apr 23 01:48:50.054: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Software che)
*Apr 23 01:48:50.154: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (DES encrypti)
Router#
*Apr 23 01:48:50.254: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (3DES encrypt)
*Apr 23 01:48:50.354: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (SHA hashing )
*Apr 23 01:48:50.454: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Random KAT t)
*Apr 23 01:48:50.674: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (AES encrypti)
*Apr 23 01:48:50.774: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (HMAC-SHA    )
Router#
*Apr 23 01:48:50.874: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (SHA256 hashi)
*Apr 23 01:48:50.974: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (SHA512 hashi)
*Apr 23 01:48:50.974: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (ALL TESTS PA)
```

test urlf cache snapshot

To save the contents of the URL filtering cache to a file, use the **test urlf cache snapshot** command in privileged EXEC mode.

test urlf cache snapshot *file-name*

Syntax Description

file-name	The name of the Cisco IOS file in which the contents of the URL filtering cache are saved. Use the Cisco IOS file system naming conventions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

To save the contents of the URL filtering cache to a file, use the **test urlf cache snapshot** command in privileged EXEC mode.

Examples

The following example shows how to save the contents of the URL filtering cache to a flash memory file system in the file trend-cache-snapshot:

```
Router# test urlf cache snapshot flash:trend-cache-snapshot
```

text-color

Note Effective with Cisco IOS Release 12.4(6)T, the **text-color** command is not available in Cisco IOS software.

To set the color of the text on the title bars of a Secure Sockets Layer Virtual Private Network (SSLVPN), use the **text-color** command in Web VPN configuration mode. To revert to the default color, use the **no** form of this command.

text-color [**black** | **white**]

no text-color [**black** | **white**]

Syntax Description

black	(Optional) Color of the text is black. This is the default value
white	(Optional) Color of the text is white.

Defaults

Color of the text is black.

Command Modes

Web VPN configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(6)T	This command was removed.

Usage Guidelines

This command is limited to only two values to limit the number of icons that are on the toolbar.

Examples

The following example shows that the text color will be white:

```
text-color white
```

Related Commands

Command	Description
webvpn	Enters Web VPN configuration mode.

throttle

To configure server group throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server, use the **throttle** command in server group configuration mode. To disable server group throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server, use the **no** form of this command.

throttle {[**accounting** *threshold*] [**access** *threshold* [**access-timeout** *number-of-timeouts*]]}

no throttle {[**accounting** *threshold*] [**access** *threshold* [**access-timeout** *number-of-timeouts*]]}

Syntax Description

accounting *threshold*	Configures the specified server group threshold value for accounting requests sent to a RADIUS server. The range is 0 through 65536. The default value is 0 (throttling disabled).
access *threshold*	Configures the specified server group threshold value for access requests sent to a RADIUS server. The range is 0 through 65536. The default value is 0 (throttling disabled).
access-timeout *number-of-timeouts*	(Optional) Specifies the number of consecutive access timeouts that are allowed before the access request from the specified server group is dropped. The range is 1 through 10. The default value is 3.

Command Default

Throttling is disabled.

Command Modes

Server-group configuration (config-sg-radius)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was implemented on the Cisco 10,000 series routers.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to configure server group throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server. Server group configurations are used to enable or disable throttling for a particular server group and to specify the threshold value for that server group.

Examples

The following examples shows how to configure server group throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server.

The following example shows how to limit the number of accounting requests sent to server-group-A to 100:

```
Router> enable
Router# configure terminal
Router(config)# aaa group server radius server-group-A
Router(config-sg-radius)# throttle accounting 100
```

The following example shows how to limit the number of access requests packets sent to server-group-A to 200 and sets the number of timeouts allowed per transactions to 2:

```
Router> enable
Router# configure terminal
Router(config)# aaa group server radius server-group-A
Router(config-sg-radius)# throttle access 200 access-timeout 2
```

The following example shows how to throttle both accounting and access request packets for server-group-A:

```
Router> enable
Router# configure terminal
Router(config)# aaa group server radius server-group-A
Router(config-sg-radius)# throttle accounting 100 access 200
```

Related Commands

Command	Description
radius-server host	Specifies a RADIUS server host.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
radius-server retransmit	Specifies the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
radius-server throttle	Configures global throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server.
radius-server timeout	Specifies the number of seconds a router waits for a server host to reply before timing out.
show radius statistics	Displays the RADIUS statistics for accounting and authentication packets.

timeout (application firewall application-configuration)

To specify the elapsed length of time before an inactive connection is torn down, use the **timeout** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

timeout *seconds*

no timeout *seconds*

Syntax Description

seconds	Idle timeout value. Available range: 5 to 43200 (12 hours).

Command Default

If this command is not issued, the default value specified via the **ip inspect tcp idle-time** command will be used.

Command Modes

cfg-appfw-policy-http configuration

cfg-appfw-policy-aim configuration

cfg-appfw-policy-ymsgr configuration

cfg-appfw-policy-msnmsgr configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	Support for the inspection of instant messenger applications was introduced.

Usage Guidelines

The **timeout** command overrides the global TCP idle timeout value for HTTP traffic or for traffic of a specified instant messenger application (AOL, Yahoo, or MSN).

Before you can issue the **timeout** command, you must enable protocol inspection via the **application** command, which allows you to specify whether you want to inspect HTTP traffic or instant messenger application traffic. The **application** command puts the router in appfw-policy-*protocol* configuration mode, where "*protocol*" is dependent upon the specified protocol.

Examples

The following example shows how to define the HTTP application firewall policy "mypolicy." This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule "firewall," which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
```

```
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
  timeout 60
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

Related Commands

Command	Description
ip inspect tcp idle-time	Specifies the TCP idle timeout (the length of time a TCP session will be managed while there is no activity).

timeout (policy group)

To configure the length of time that an end user session can remain idle or the total length of time that the session can remain connected, use the **timeout** command in webvpn group policy configuration mode. To configure timeout timers to default values, use the **no** form of this command.

timeout {**idle** *seconds* | **session** *seconds*}

no timeout {**idle** | **session**}

Syntax Description

idle *seconds*	Configures the length time that an end user connection can remain idle.
session *seconds*	Configures the total length of time that an end user can maintain a single connection.

Command Default

The following default values are used if this command is not configured or if the **no** form is entered:

idle 2100
session 43200

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command is used to configure the idle or session timer value. The idle timer sets the length of time that a session will remain connected when the end user generates no activity. The session timer sets the total length of time that a session will remain connected, with or without activity. Upon expiration of either timer, the end user connection is closed. The user must login or reauthenticate to access the Secure Sockets Layer Virtual Private Network (SSL VPN).

Note The idle timer is not the same as the dead peer timer. The dead peer timer is reset when any packet type is received over the Cisco AnyConnect VPN Client tunnel. The idle timer is reset only when the end user generates activity.

Examples

The following example sets the idle timer to 30 minutes and session timer to 10 hours:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# timeout idle 1800
Router(config-webvpn-group)# timeout session 36000
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

timeout file download

To specify how often the consent webpage should be downloaded from the file server, use the **timeout file download** command in parameter-map-type consent configuration mode. To remove the configured download time, use the **no** form of this command with the configured time.

timeout file download *minutes*

no timeout file download *minutes*

Syntax Description

minutes	The time, in minutes, that specifies how often the consent webpage should be downloaded from the file server. Available range: 1 to 525600.

Command Default

The consent webpage is not downloaded from the file server.

Command Modes

Parameter-map-type consent (config-profile)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Using the **timeout file download** command ensures that the consent file has the most current parameter map defintions.

Examples

In the following example, the file “consent_page.html” will be downloaded from the file server every 35791 minutes:

```
parameter-map type consent consent_parameter_map
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity consent_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
parameter-map type consent default
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity test_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
```

timeout login response

To specify how long the system will wait for login input (such as username and password) before timing out, use the **timeout login response** command in line configuration mode. To set the timeout value to 30 seconds (which is the default timeout value), use the **no** form of this command.

timeout login response *seconds*

no timeout login response *seconds*

Syntax Description

seconds	Integer that determines the number of seconds the system will wait for login input before timing out. Available settings are from 1 to 300 seconds. The default value is 30 seconds.

Defaults

The default login timeout value is 30 seconds.

Command Modes

Line configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example changes the login timeout value to 60 seconds:

```
line 10
 timeout login response 60
```

timeout retransmit

To set an interval for a router to wait for a reply from the Lightweight Directory Access Protocol (LDAP) server before it times out, use the **timeout retransmit** command in LDAP server configuration. To restore the default, use the **no** form of this command.

timeout retransmit *seconds*

no timeout retransmit *seconds*

Syntax Description

seconds	The timeout interval, in seconds. The range is from 1 to 65535. The default is 30.

Command Default

The default timeout interval value is 30 seconds.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

The recommended value to configure the LDAP server to timeout is 30 seconds.

Examples

The following example shows how to set an interval timer of 20 seconds for the LDAP server:

```
Router(config)# ldap server server1
Router(config-ldap-server)# timeout retransmit 20
```

Related Commands

Command	Description
ipv4(ldap)	Creates an IPv4 address within an LDAP server address pool.
ldap server	Defines an LDAP server and enters LDAP server configuration mode.
transport port (**ldap**)	Configures the transport protocol for establishing a connection with the LDAP server.

timer (Diameter peer)

To configure the Diameter Credit Control Application (DCCA) for peer-to-peer communication, use the **timer** command in Diameter peer configuration mode. To disable the configured protocol, use the **no** form of this command.

timer {**connection** | **transaction** | **watchdog**} *value*

no timer {**connection** | **transaction** | **watchdog**} *value*

Syntax Description

connection	Maximum interval, in seconds, for the Gateway General Packet RadioService (GPRS) Support Node (GGSN) to attempt reconnection to a Diameter peer after after being disconnected because of a transport failure. The range is from 1 to 1000. The default is 30. A value of 0 configures the GGSN not to attempt reconnection.
transaction	Maximum interval, in seconds, the GGSN waits for a Diameter peer to respond before trying another peer. The range is from 1 to 1000. The default is 30.
watchdog	Maximum interval, in seconds, the GGSN waits for a Diameter peer response to a watchdog packet. The range is from 1 to 1000. The default is 30. **Note** When the watchdog timer expires, a device watchdog request (DWR) is sent to the Diameter peer and the watchdog timer is reset. If a device watchdog answer (DWA) is not received before the next expiration of the watchdog timer, a transport failure to the Diameter peer has occurred.
value	The valid range, in seconds, from 1 to 1000. The default is 30.

Command Default

The default for each timer is 30 seconds.

Command Modes

Diameter peer configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

When configuring timers, the value for the transaction timer should be larger than the transmission-timeout value, and, on the Serving GPRS Support Node (SGSN), the values configured for the number of GPRS Tunneling Protocol (GTP) N3 requests and T3 retransmissions must be larger than the sum of all possible server timers (RADIUS, Diameter Credit Control Application (DCCA), and Cisco Content Services Gateway (CSG)). Specifically, the SGSN N3*T3 must be greater than 2 x RADIUS timeout + *N* x DCCA timeout + CSG timeout where:

- The factor *2* is for both authentication and accounting.
- The value *N* is for the number of Diameter servers configured in the server group.

Examples

The following example shows how to configure the Diameter base protocol timers for a Diameter peer:

```
Router (config-dia-peer)# timer connection 20
Router (config-dia-peer)# timer watchdog 25
```

Related Commands

Command	Description
diameter peer	Configures a Diameter peer and enters Diameter peer configuration sub-mode.
diameter peer timer	Configures the Diameter base protocol timers globally.

timers delay

To configure the time that a redundancy group takes to delay role negotiations that start after a fault occurs or the system is reloaded, use the **timers delay** command in redundancy application group configuration mode**.** To disable the timer, use the **no** form of this command.

timers delay *seconds* [**reload** *seconds*]

no timers delay *seconds* [**reload** *seconds*]

Syntax Description

seconds	Delay value. The range is from 0 to 10000. The default is 10.
reload	(Optional) Specifies the redundancy group reload timer.
seconds	(Optional) Reload timer value in seconds. The range is from 0 to 10000. The default is 120.

Command Default

The default is 10 seconds for timer delay and 120 seconds for reload delay.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following example shows how to set the timer delay value and reload value for a redundancy group named group 1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# timers delay 100 reload 400
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
control	Configures the control interface type and number for a redundancy group.
data	Configures the data interface type and number for a redundancy group.
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.

Command	Description
protocol	Defines a protocol instance in a redundancy group.
redundancy rii	Configures the RII for the redundancy group.

timers hellotime

To configure timers for hellotime and holdtime messages for a redundancy group, use the **timers hellotime** command in redundancy application protocol configuration mode**.** To disable the timers in the redundancy group, use the **no** form of this command.

timers hellotime [**msec**] *seconds* **holdtime** [**msec**] *seconds*

no timers hellotime [**msec**] *seconds* **holdtime** [**msec**] *seconds*

Syntax Description

msec	(Optional) Specifies the interval, in milliseconds, for hello messages.
seconds	Interval time, in seconds, for hello messages. The range is from 1 to 254.
holdtime	Specifies the hold timer.
msec	Specifies the interval, in milliseconds, for hold time messages.
seconds	Interval time, in milliseconds, for hold time messages. The range is from 6 to 255.

Command Default

The default value for the hellotime interval is 3 seconds and for the holdtime interval is 10 seconds.

Command Modes

Redundancy application protocol configuration (config-red-app-prtc)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The hello time is an interval in which hello messages are sent. The holdtime is the time before the active or the standby device is declared to be in down state. Use the **msec** keyword to configure the timers in milliseconds.

Examples

The following example shows how to configure the hellotime and holdtime messages:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# protocol 1
Router(config-red-app-prtcl)# timers hellotime 100 holdtime 100
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.
protocol	Defines a protocol instance in a redundancy group.

title

To configure the HTML title string that is shown in the browser title and on the title bar of a Secure Sockets Layer Virtual Private Network (SSL VPN), use the **title** command in webvpn context configuration mode. To revert to the default text string, use the **no** form of this command.

title [*title-string*]

no title [*title-string*]

Syntax Description

title-string	(Optional) Title string, up to 255 characters in length, that is displayed in the browser of the user. The string value may contain 7-bit ASCII characters, HTML tags, and escape sequences.

Defaults

If this command is not configured or if the **no** form is entered, the following text is displayed:

"WebVPN Service"

Command Modes

Webvpn context configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The optional form of the **title** command is entered to configure a custom text string. If this command is issued without entering a text string, a title will not be displayed in the browser window. If the **no** form of this command is used, the default title string "WebVPN Service" is displayed.

Examples

The following example configures "Secure Access: Unauthorized users prohibited" as the title string:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# title "Secure Access: Unauthorized users prohibited"
Router(config-webvpn-context)#
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

title-color

To specify the color of the title bars on the login and portal pages of a Secure Sockets Layer Virtual Private Network (SSL VPN), use the **title-color** command in webvpn context configuration mode. To remove the color, use the **no** form of this command.

title-color *color*

no title-color *color*

Syntax Description

color	The value for the *color* argument is entered as a comma-separated red, green, blue (RGB) value, an HTML color value (beginning with a"#"), or the name of the color that is recognized in HTML (no spaces between words or characters). The value is limited to 32 characters. The value is parsed to ensure that it matches one of the following formats (using Perl regex notation): • \#/x{6} • \d{1,3},\d{1,3},\d{1,3} (and each number is from 1 to 255) • \w+ The default is purple.

Defaults

The color purple is used if this command is not configured or if the **no** form is entered.

Command Modes

Webvpn context configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(6)T	Support for the SSL VPN enhancements feature was added.

Usage Guidelines

Configuring a new color overrides the color the preexisting color.

Examples

The following examples show the three command forms that can be used to configure the title color:

```
Router(config-webvpn-context)# title-color darkseagreen
Router(config-webvpn-context)# title-color #8FBC8F
Router(config-webvpn-context)# title-color 143,188,143
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

track (firewall)

To configure the redundancy group tracking, use the **track** command in redundancy application group configuration mode**.** To remove the redundancy group tracking, use the **no** form of this command.

track *object-number* {**decrement** *value* | **shutdown**}

no track *object-number* {**decrement** *value* | **shutdown**}

Syntax Description

object-number	ID of the event type.
decrement *value*	Specifies the value that the priority will be decremented. The range is from 1 to 255.
shutdown	Shuts down a redundancy group if the tracked object goes down instead of changing the priority.

Command Default

Objects and decrement priority per object are not tracked.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The redundancy group can track an object and decrease the priority value per object. Multiple objects can be tracked by the redundancy group to influence the priority appropriately. You can shut down a redundancy group if the tracked object goes down instead of changing the priority.

Examples

The following example shows how to track the redundancy group named group1 and assign a decrement value:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# track 200 decrement 50
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.

Command	Description
control	Configures the control interface type and number for a redundancy group.
data	Configures the data interface type and number for a redundancy group.
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.
protocol	Defines a protocol instance in a redundancy group.
redundancy rii	Configures the RII for the redundancy group.

traffic-export

To control the operation of IP traffic capture mode in IP traffic export, use the **traffic-export** command in privileged EXEC mode.

traffic-export interface *type number* { **start** | **stop** | **clear** | **copy** *memory-device* }

Syntax Description

type number	Type and number of the interface over which the packets being captured travel.
start	Initiates a packet capture sequence.
stop	Halts a packet capture sequence.
clear	Clears the packet capture buffer.
copy	Copies the contents of the packet capture buffer to an external device.
memory-device	External memory device to which captured packets are transmitted. Options are *flash:*, *tftp:*, or *usbflash0:*.

Command Default

This command has no defaults.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **traffic-export** command to control the operation of IP traffic capture mode in IP traffic export. The operator uses CLI commands to start or stop capture of packets flowing across a monitored interface, to copy the captured packets to an external memory device, or to clear the internal buffer which holds the captured packets.

Examples

The following example illustrates the use of the **traffic-export** command to initiate the capture of packets on interface FastEthernet 0/0.

```
Router# traffic-export interface fastethernet 0/0 start
%RITE-5-CAPTURE_START: Started IP traffic capture for interface FastEthernet0/0
router#
```

The following example illustrates the use of the **traffic-export** command to halt the packet capture sequence on interface FastEthernet 0/0.

```
Router# traffic-export interface fastethernet 0/0 stop
```

```
%RITE-5-CAPTURE_STOP: Stopped IP traffic capture for interface FastEthernet0/0
router#
```

The following example illustrates the use of the **traffic-export** command to copy the contents of the packet capture buffer to an external memory device. The example of the interactive dialog identifies the external memory device and the remote host in which it resides.

```
Router# traffic-export interface fastethernet0/0 copy tftp:
Address or name of remote host []? 172.18.207.15
Capture buffer filename []? atmcapture
Copying capture buffer to tftp://172.18.207.15/atmcapture !!
router#
```

The following example illustrates the use of the **traffic-export** command to clear the packet capture buffer that is in local memory.

```
Router# traffic-export interface fastethernet 0/0 clear
%RITE-5-CAPTURE_CLEAR: Cleared IP traffic capture buffer for interface FastEthernet0/0

router#
```

Related Commands

Command	Description
ip traffic-export apply profile	Applies an IP traffic export or IP traffic capture profile to a specific interface.
ip traffic-export profile	Creates an IP traffic export or IP traffic capture profile on an ingress interface.

transfer-encoding type

To permit or deny HTTP traffic according to the specified transfer-encoding of the message, use the **transfer-encoding type** command in appfw-policy-http configuration mode. To disable this inspection parameter, use the **no** form of this command.

transfer-encoding type {**chunked** | **compress** | **deflate** | **gzip** | **identity** | **default**} **action** {**reset** | **allow**} [**alarm**]

no transfer-encoding type {**chunked** | **compress** | **deflate** | **gzip** | **identity** | **default**} **action** {**reset** | **allow**} [**alarm**]

Syntax Description

chunked	Encoding format (specified in RFC 2616, *Hypertext Transfer Protocol—HTTP/1*) in which the body of the message is transferred in a series of chunks; each chunk contains its own size indicator.
compress	Encoding format produced by the UNIX "compress" utility.
deflate	"ZLIB" format defined in RFC 1950, *ZLIB Compressed Data Format Specification version 3.3*, combined with the "deflate" compression mechanism described in RFC 1951, *DEFLATE Compressed Data Format Specification version 1.3*.
gzip	Encoding format produced by the "gzip" (GNU zip) program.
identity	Default encoding, which indicates that no encoding has been performed.
default	All of the transfer encoding types.
action	Encoding types outside of the specified type are subject to the specified action (**reset** or **allow**).
reset	Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection.
allow	Forwards the packet through the firewall.
alarm	(Optional) Generates system logging (syslog) messages for the given action.

Defaults

If a given type is not specified, all transfer-encoding types are supported with the reset alarm action.

Command Modes

appfw-policy-http configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Only encoding types specified by the **transfer-encoding-type** command are allowed through the firewall.

Examples

The following example shows how to define the HTTP application firewall policy “mypolicy.” This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule “firewall,” which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

transport port

To configure the transport protocol for establishing a connection with the Diameter peer, use the **transport port** command in Diameter peer configuration mode. To block all sessions that are bound to the peer from using the connection, use the **no** form of this command.

transport tcp port *port-number*

no transport tcp port *port-number*

Syntax Description

tcp	Currently, TCP is the only supported transport protocol for establishing the connection with the Diameter peer.
port-number	Character string identifying the peer connection port.

Command Default

TCP is the default transport protocol.

Command Modes

Diameter peer configuration

Command History

Release	Modification
12.4(9)T	This command was introduced .

Examples

The following example configures TCP as the transport protocol and port 4100 as the peer connection port:

```
Router (config-dia-peer)# transport tcp port 4100
```

Related Commands

Command	Description
diameter peer	Defines a Diameter peer and enters Diameter peer configuration mode.

transport port (ldap)

To configure the transport protocol for establishing a connection with the Lightweight Directory Access Protocol (LDAP) server, use the **transport port** command in LDAP server configuration mode. To delete all sessions that are bound to the server from using the connection, use the **no** form of this command.

transport port *port-number*

no transport port *port-number*

Syntax Description

port-number	Server connection port number. Valid port numbers range from 1 to 65535. The default is 389.

Command Default

The default port number is 389.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Examples

The following example shows how to configure the transport protocol and port 200 as the peer connection port:

```
Router(config)# ldap server server1
Router(config-ldap-server)# transport port 200
```

Related Commands

Command	Description
ipv4 (**ldap**)	Creates an IPv4 address within an LDAP server address pool.
ldap server	Defines an LDAP server and enters LDAP server configuration mode.

trm register

To allow the user to manually register the platform with the Trend Router Provisioning Server (TRPS), use the **trm register** command in privileged EXEC mode.

trm register[**force**]

Syntax Description

force	Sends a new registration request to TRPS.

Command Default

This command is not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
15.1(2)T	This command was modified. The **force** keyword was added.

Usage Guidelines

Use the **trm register** command to enable manual registration of the platform with the TRPS. If you do not use this command, the system sends a registration request to the TRPS every minute after boot-up until the registration is successful.

Examples

The following is sample output from the **trm register** command:

```
Router# trm register

Processing registration request.
Please run ‘show ip trm subscription” status to get more info
```

trustpoint (tti-petitioner)

To specify the trustpoint that is to be associated with the Trusted Transitive Introduction (TTI) exchange between the Secure Device Provisioning (SDP) petitioner and the SDP registrar, use the **trustpoint** command in tti-petitioner configuration mode. To change the specified trustpoint or use the default trustpoint, use the **no** form of this command.

trustpoint *trustpoint-label*

no trustpoint *trustpoint-label*

Syntax Description

trustpoint-label	Name of trustpoint.

Defaults

If a trustpoint is not specified, a default trustpoint called “tti” is generated.

Command Modes

tti-petitioner configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the **trustpoint** command in tti-petitioner configuration mode to associate a trustpoint with the SDP petitioner.

Examples

The following example shows how specify the trustpoint “mytrust”:

```
crypto wui tti petitioner
 trustpoint mytrust
```

After the SDP exchange is complete, the petitioner will automatically enroll with the registrar and obtain a certificate. The following sample output from the **show running-config** command shows an automatically generated configuration which generates the default trustpoint “tti”:

```
crypto pki trustpoint tti
 enrollment url http://pki1-36a.cisco.com:80
 revocation-check crl
 rsakeypair tti 1024
 auto-enroll 70
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
crypto wui tti petitioner	Configures a device to become an SDP petitioner and enters tti-petitioner configuration mode.

trustpoint signing

To specify the trustpoint and associated certificate to be used when signing all introduction data during the Secure Device Provisioning (SDP) exchange, use the **trustpoint signing** command in tti-petitioner configuration mode. To change the specified trustpoint or use the default trustpoint, use the **no** form of this command.

trustpoint signing *trustpoint-label*

no trustpoint signing *trustpoint-label*

Syntax Description

trustpoint-label	Name of trustpoint.

Defaults

If a trustpoint is not specified, any existing device certificate is used. If none is available, a self-signed certificate is generated.

Command Modes

tti-petitioner configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use the **trustpoint signing** command in tti-petitioner configuration mode to associate a specific trustpoint with the petitioner for signing its certificate.

Examples

The following example shows how to specify the trustpoint mytrust:

```
crypto provisioning petitioner
 trustpoint signing mytrust
```

After the SDP exchange is complete, the petitioner automatically enrolls with the registrar and obtains a certificate. The following sample output from the **show running-config** command shows an automatically generated configuration with the default trustpoint tti:

```
crypto pki trustpoint tti
 enrollment url http://pki1-36a.cisco.com:80
 revocation-check crl
 rsakeypair tti 1024
 auto-enroll 70
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
crypto provisioning petitioner	Configures a device to become an SDP petitioner and enters tti-petitioner configuration mode.
trustpoint (tti-petitioner)	Specifies the trustpoint associated with the SDP exchange between the petitioner and the registrar.

tunnel mode

To set the encapsulation mode for the tunnel interface, use the **tunnel mode** command in interface configuration mode. To restore the default mode, use the **no** form of this command.

tunnel mode {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **gre multipoint** | **gre ipv6** | **ipip** [**decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6** | **ipsec ipv6** | **mpls** | **nos** | **rbscp**}

no tunnel mode

Syntax Description

aurp	AppleTalk Update-Based Routing Protocol.
cayman	Cayman TunnelTalk AppleTalk encapsulation.
dvmrp	Distance Vector Multicast Routing Protocol.
eon	EON compatible Connectionless Network Protocol (CLNS) tunnel.
gre	Generic routing encapsulation (GRE) protocol. This is the default.
gre multipoint	Multipoint GRE (mGRE).
gre ipv6	GRE tunneling using IPv6 as the delivery protocol.
ipip	IP-over-IP encapsulation.
decapsulate-any	(Optional) Terminates any number of IP-in-IP tunnels at one tunnel interface. This tunnel will not carry any outbound traffic; however, any number of remote tunnel endpoints can use a tunnel configured this way as their destination.
ipsec ipv4	Tunnel mode is IPSec, and the transport is IPv4.
iptalk	Apple IPTalk encapsulation.
ipv6	Static tunnel interface configured to encapsulate IPv6 or IPv4 packets in IPv6.
ipsec ipv6	Tunnel mode is IPSec, and the transport is IPv6.
mpls	Multiprotocol Label Switching (MPLS) encapsulation.
nos	KA9Q/NOS compatible IP over IP.
rbscp	Rate Based Satellite Control Protocol (RBSCP).

Command Default

The default is GRE tunneling.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
10.3	The **aurp**, **dvmrp**, and **ipip** keywords were added.
11.2	The optional **decapsulate-any** keyword was added.
12.2(13)T	The **gre multipoint** keyword was added.

Release	Modification
12.3(7)T	The following keywords were added: • **gre ipv6** to support GRE tunneling using IPv6 as the delivery protocol. • **ipv6** to allow a static tunnel interface to be configured to encapsulate IPv6 or IPv4 packets in IPv6. • **rbscp** to support RBSCP.
12.3(14)T	The **ipsec ipv4** keyword was added.
12.2(18)SXE	The **gre multipoint** keyword added.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.4(4)T	The **ipsec ipv6** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Source and Destination Address

You cannot have two tunnels that use the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and source packets off of the loopback interface.

Cayman Tunneling

Designed by Cayman Systems, Cayman tunneling implements tunneling to enable Cisco routers to interoperate with Cayman GatorBoxes. With Cayman tunneling, you can establish tunnels between two routers or between a Cisco router and a GatorBox. When using Cayman tunneling, you must not configure the tunnel with an AppleTalk network address.

DVMRP

Use DVMRP when a router connects to an mrouted (multicast) router to run DVMRP over a tunnel. You must configure Protocol Independent Multicast (PIM) and an IP address on a DVMRP tunnel.

GRE with AppleTalk

GRE tunneling can be done between Cisco routers only. When using GRE tunneling for AppleTalk, you configure the tunnel with an AppleTalk network address. Using the AppleTalk network address, you can ping the other end of the tunnel to check the connection.

Multipoint GRE

After enabling mGRE tunneling, you can enable the **tunnel protection** command, which allows you to associate the mGRE tunnel with an IPSec profile. Combining mGRE tunnels and IPSec encryption allows a single mGRE interface to support multiple IPSec tunnels, thereby simplifying the size and complexity of the configuration.

Note GRE tunnel keepalives configured using the **keepalive** command under a GRE interface are supported only on point-to-point GRE tunnels.

RBSCP

RBSCP tunneling is designed for wireless or long-distance delay links with high error rates, such as satellite links. Using tunnels, RBSCP can improve the performance of certain IP protocols, such as TCP and IPSec, over satellite links without breaking the end-to-end model.

IPSec in IPv6 Transport

IPv6 IPSec encapsulation provides site-to-site IPSec protection of IPv6 unicast and multicast traffic. This feature allows IPv6 routers to work as a security gateway, establishes IPSec tunnels between another security gateway router, and provides crypto IPSec protection for traffic from an internal network when being transmitting across the public IPv6 Internet. IPv6 IPSec is very similar to the security gateway model using IPv4 IPsec protection.

Examples

Cayman Tunneling

The following example shows how to enable Cayman tunneling:

```
Router(config)# interface tunnel 0
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode cayman
```

GRE Tunneling

The following example shows how to enable GRE tunneling:

```
Router(config)# interface tunnel 0
Router(config-if)# appletalk cable-range 4160-4160 4160.19
Router(config-if)# appletalk zone Engineering
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode gre
```

IPSec in IPv4 Transport

The following example shows how to configure a tunnel using IPSec encapsulation with IPv4 as the transport mechanism:

```
Router(config)# crypto ipsec profile PROF
Router(config)#  set transform tset
Router(config)# interface Tunnel0
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# tunnel mode ipsec ipv4
Router(config-if)# tunnel source Loopback0
Router(config-if)# tunnel destination 172.16.1.1
Router(config-if)# tunnel protection ipsec profile PROF
```

IPSec in IPv6 Transport

The following example shows how to configure an IPv6 IPSec tunnel interface:

```
Router(config)# interface tunnel 0
Router(config-if)# ipv6 address 2001:0DB8:1111:2222::2/64
Router(config-if)# tunnel destination 10.0.0.1
Router(config-if)# tunnel source Ethernet 0/0
Router(config-if)# tunnel mode ipsec ipv6
Router(config-if)# tunnel protection ipsec profile profile1
```

Multipoint GRE Tunneling

The following example shows how to enable mGRE tunneling:

```
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
! Ensures longer packets are fragmented before they are encrypted; otherwise, the
! receiving router would have to do the reassembly.
 ip mtu 1416
! Turns off split horizon on the mGRE tunnel interface; otherwise, EIGRP will not
! advertise routes that are learned via the mGRE interface back out that interface.
 no ip split-horizon eigrp 1
 no ip next-hop-self eigrp 1
 delay 1000
! Sets IPSec peer address to Ethernet interface's public address.
 tunnel source Ethernet0
 tunnel mode gre multipoint
! The following line must match on all nodes that want to use this mGRE tunnel.
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
```

RBSCP Tunneling

The following example shows how to enable RBSCP tunneling:

```
Router(config)# interface tunnel 0
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode rbscp
```

Related Commands

Command	Description
appletalk cable-range	Enables an extended AppleTalk network.
appletalk zone	Sets the zone name for the connected AppleTalk network.
tunnel destination	Specifies the destination for a tunnel interface.
tunnel protection	Associates a tunnel interface with an IPSec profile.
tunnel source	Sets the source address of a tunnel interface.

tunnel protection

To associate a tunnel interface with an IP Security (IPSec) profile, use the **tunnel protection** command in interface configuration mode. To disassociate a tunnel with an IPSec profile, use the **no** form of this command.

tunnel protection ipsec profile *name* [**shared**]

no tunnel protection ipsec profile *name* [**shared**]

Syntax Description

ipsec profile	Enables generic routing encapsulation (GRE) tunnel encryption via IPSec.
name	Name of the IPSec profile. This value must match the *name* specified in the **crypto ipsec profile** command.
shared	(Optional) Allows the tunnel protection IPSec Security Association Database (SADB) to share the same dynamic crypto map instead of creating a unique crypto map per tunnel interface. **Note** Unlike the **tunnel protection** command, which specifies that IPSec encryption will be performed after GRE encapsulation, configuring a crypto map on a tunnel interface specifies that encryption will be performed before GRE encapsulation. **Note** If the **shared** keyword is used, the **tunnel source** command must specify an interface instead of an IP address. Crypto sockets are not shared if the tunnel source is not specified as an interface.

Defaults

Tunnel interfaces are not associated with IPSec profiles.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.3(5)T	The shared keyword was added through DDTS CSCec28392.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.4(5)	The **shared** keyword was changed so that if it is used with the **tunnel protection** command, the **tunnel source** command must specify an interface instead of an IP address.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

Use the **tunnel protection** command to specify that IPSec encryption will be performed after the GRE has been added to the tunnel packet. The **tunnel protection** command can be used with multipoint GRE (mGRE) and point-to-point GRE (p-pGRE) tunnels. With p-pGRE tunnels, the tunnel destination address will be used as the IPSec peer address. With mGRE tunnels, multiple IPSec peers are possible; the corresponding Next Hop Resolution Protocol (NHRP) mapping nonbroadcast multiaccess (NBMA) destination addresses will be used as the IPSec peer addresses.

The shared Keyword

If you want to configure two Dynamic Multipoint VPN (DMVPN) mGRE and IPSec tunnels on the same router with the same local endpoint (tunnel source) configuration, you *must* issue the **shared** keyword.

The dynamic crypto map that is created by the **tunnel protection** command is always different from a crypto map that is configured directly on the interface.

Note GRE tunnel keepalives (configured with the **keepalive** command under the GRE interface) are not supported in combination with the **tunnel protection** command.

Examples

The following example shows how to associate the IPSec profile "vpnprof" with an mGRE tunnel interface. In this example, the IPSec source peer address will be the IP address from Ethernet interface 0. There is a static NHRP mapping from IP address 10.0.0.3 to IP address 172.16.2.1, so for this NHRP mapping the IPSec destination peer address will be 172.16.2.1. The IPSec proxy will be as follows: **permit gre host** *ethernet0-ip-address* **host** *ip-address*. Other NHRP mappings (static or dynamic) will automatically create additional IPSec security associations (SAs) with the same source peer address and the destination peer address from the NHRP mapping. The IPSec proxy for these NHRP mappings will be as follows: **permit gre host** *ethernet0-ip-address* **host** *NHRP-mapping-NBMA-address*.

```
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
! Ensures that longer packets are fragmented before they are encrypted; otherwise, the
! receiving router would have to do the reassembly.
 ip mtu 1416
 ip nhrp authentication donttell
 ip nhrp map multicast dynamic
 ip nhrp network-id 99
 ip nhrp holdtime 300
! Turns off split horizon on the mGRE tunnel interface; otherwise, EIGRP will not
! advertise routes that are learned via the mGRE interface back out that interface.
 no ip split-horizon eigrp 1
 no ip next-hop-self eigrp 1
 delay 1000
! Sets the IPSec peer address to the Ethernet interface's public address.
 tunnel source Ethernet0
 tunnel mode gre multipoint
! The following line must match on all nodes that want to use this mGRE tunnel.
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
```

The following example shows how to associate the IPSec profile "vpnprof" with a p-pGRE tunnel interface. In this example, the IPSec source peer address will be the IP address from Ethernet interface 0. The IPSec destination peer address will be 172.16.1.10 (per the **tunnel destination** *address* command). The IPSec proxy will be as follows: **permit gre host** *ethernet0-ip-address* **host** *ip-address*.

```
interface Tunnel1
 ip address 10.0.1.1 255.255.255.252
! Ensures that longer packets are fragmented before they are encrypted; otherwise, the
! receiving router would have to do the reassembly.
 ip mtu 1420
 tunnel source Ethernet0
 tunnel destination 172.16.1.10
 tunnel protection ipsec profile vpnprof
```

In the following example, the crypto sockets are shared between the Tunnel0 and Tunnel1 interfaces because the **tunnel protection** command on both interfaces uses the same profile and is configured with the **shared** keyword. Both tunnels specify the tunnel source to be an Ethernet0/0 interface.

```
interface Tunnel0
ip address 10.255.253.3 255.255.255.0
no ip redirects
ip mtu 1436
ip nhrp authentication h1there
ip nhrp map 10.255.253.1 192.168.1.1
ip nhrp map multicast 192.168.1.1
ip nhrp network-id 253
ip nhrp holdtime 600
ip nhrp nhs 10.255.253.1
ip ospf message-digest-key 1 md5 wellikey
ip ospf network broadcast
ip ospf cost 35
ip ospf priority 0
no ip mroute-cache
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel key 253
tunnel protection ipsec profile dmvpn-profile shared


interface Tunnel1
ip address 10.255.254.3 255.255.255.0
no ip redirects
ip mtu 1436
ip nhrp authentication h1there
ip nhrp map multicast 192.168.1.3
ip nhrp map 10.255.254.1 192.168.1.3
ip nhrp network-id 254
ip nhrp holdtime 600
ip nhrp nhs 10.255.254.1
ip ospf message-digest-key 1 md5 wellikey
ip ospf network broadcast
ip ospf priority 0
no ip mroute-cache
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel key 254
tunnel protection ipsec profile dmvpn-profile shared
```

Related Commands

Command	Description
crypto ipsec profile	Defines the IPSec parameters that are to be used for IPSec encryption between two IPSec routers.
interface	Configures an interface type and enters interface configuration mode.
keepalive (tunnel interfaces)	Enables keepalive packets and specifies the number of times that the Cisco IOS software tries to send keepalive packets without a response before bringing the tunnel protocol down for a specific interface.
permit	Sets conditions for a named IP access list.
tunnel source	Sets the source address for a tunnel interface.

type echo protocol ipIcmpEcho

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SRB, 12.2(33)SB, and 12.2(33)SXI, the **type echo protocol ipIcmpEcho** command is replaced by the **icmp-echo** command. See the **icmp-echo** command for more information.

To configure an IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) echo operation, use the **type echo protocol ipIcmpEcho** command in IP SLA monitor configuration mode.

type echo protocol ipIcmpEcho {*destination-ip-address* | *destination-hostname*} [**source-ipaddr** {*ip-address* | *hostname*} | **source-interface** *interface-name*]

Syntax Description

destination-ip-address | *destination-hostname*	Destination IP address or hostname for the operation.
source-ipaddr {*ip-address* | *hostname*}	(Optional) Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.
source-interface *interface-name*	(Optional) Specifies the source interface for the operation.

Defaults

No IP SLAs operation type is configured for the operation being configured.

Command Modes

IP SLA monitor configuration (config-sla-monitor)

Command History

Release	Modification
11.2	This command was introduced.
12.0(5)T	The following keyword and arguments were added: • **source-ipaddr** {*ip-address* | *hostname*}
12.3(7)XR	The **source-interface** keyword and *interface-name* argument were added.
12.3(11)T	The **source-interface** keyword and *interface-name* argument were added.
12.4(4)T	This command was replaced by the **icmp-echo** command.
12.2(33)SRB	This command was replaced by the **icmp-echo** command.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was replaced by the **icmp-echo** command.
12.2(33)SXI	This command was replaced by the **icmp-echo** command.

Usage Guidelines

The default request packet data size for an ICMP echo operation is 28 bytes. Use the **request-data-size** command to modify this value. This data size is the payload portion of the ICMP packet, which makes a 64-byte IP packet.

You must configure the type of IP SLAs operation (such as User Datagram Protocol [UDP] jitter or Internet Control Message Protocol [ICMP] echo) before you can configure any of the other parameters of the operation. To change the operation type of an existing IP SLAs operation, you must first delete the IP SLAs operation (using the **no ip sla monitor** global configuration command) and then reconfigure the operation with the new operation type.

Examples

In the following example, IP SLAs operation 10 is created and configured as an echo operation using the IP/ICMP protocol and the destination IP address 172.16.1.175.

```
ip sla monitor 10
 type echo protocol ipIcmpEcho 172.16.1.175
!
ip sla monitor schedule 10 start-time now
```

Related Commands

Command	Description
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.

udp idle-time

To configure the idle timeout of User Datagram Protocol (UDP) sessions going through the firewall, use the **udp idle-time** command in parameter-map type inspect configuration mode. To disable this function, use the **no** form of this command.

udp idle-time *seconds*

no udp idle-time *seconds*

Syntax Description

seconds	Amount of time, in seconds, for which a UDP session will continue to be managed while there is no activity.

Command Default

None

Command Modes

Parameter-map type inspect configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

When you are configuring an inspect type parameter map, you can enter the **udp idle-time** subcommand after you enter the **parameter-map type inspect** command.

When the software detects a valid UDP packet, the software establishes state information for a new UDP session. Because UDP is a connectionless service, there are no actual sessions, so the software approximates sessions by examining the information in the packet and determining if the packet is similar to other UDP packets (for example, it has similar source or destination addresses) and if the packet was detected soon after another similar UDP packet.

If the software detects no UDP packets for the UDP session for the a period of time defined by the UDP idle timeout, the software will not continue to manage state information for the session.

For more detailed information about creating a parameter map, see the **parameter-map type inspect** command.

Examples

The following example specifies that if there is no activity, the UDP session will continue to be managed for 75 seconds:

```
parameter-map type inspect eng-network-profile
 udp idle-time 75
```

Related Commands

Command	Description
ip inspect udp idle-time	Specifies the UDP idle timeout (the length of time for which a UDP session will still be managed while there is no activity).
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

unmatched-action

To define the action when the user request does not match the IP address or host site configuration, use the **unmatched-action** command in URL rewrite configuration mode. To disable the action, use the **no** form of this command.

unmatched-action [**direct-access** | **redirect**]

no unmatched-action [**direct-access** | **redirect**]

Syntax Description

direct-access	(Optional) Provides direct access to the URL and an information page stating that the user can access the URL directly.
redirect	(Optional) Provides the user with direct access to the URL, but the user does not receive the information page as with the **direct-access** keyword.

Command Default

Direct access to the URL

Command Modes

URL rewrite configuration (config-webvpn-url-rewrite)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example shows that the user has direct access to the URL:

```
Router (config)# webvpn context
Router (config-webvpn-context)# url rewrite
Router (config-webvpn-url-rewrite)# unmatched-action direct-access
```

Related Commands

Command	Description
host (webvpn url rewrite)	Selects the hostname of the site to be mangled on an SSL VPN gateway.
ip (webvpn url rewrite)	Configures the IP address of the site to be mangled on an SSL VPN gateway.

url (ips-auto-update)

To define a location in which to retrieve the Cisco IOS Intrusion Prevention System (IPS) signature configuration files, use the **url** command in IPS-auto-update configuration mode.

url *url*

Syntax Description

url	Location in which the router retrieves the latest signature files.

Command Default

The default value is defined in the signature definition XML.

Command Modes

IPS-auto-update configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Automatic signature updates allow users to override the existing IPS configuration and automatically keep signatures up to date on the basis of a preset time, which can be configured to a preferred setting.

Examples

In this example, the signature package file is pulled from the TFTP server at the start of every hour or every day, Sunday through Thursday. (Note that adjustments are made for months without 31 days and daylight savings time.)

```
Router# show ip ips auto-update

IPS Auto Update Configuration
    URL : tftp://192.168.0.2/jdoe/ips-auto-update/IOS_reqSeq-dw.xml
    Username : not configured
    Password : not configured
    Auto Update Intervals
      minutes (0-59) : 0
      hours (0-23) : 0-23
      days of month (1-31) : 1-31
      days of week: (0-6) : 1-5
```

Related Commands

Command	Description
ip ips auto-update	Enables automatic signature updates for Cisco IOS IPS.

url rewrite

To mangle selective URL requests on a Secure Socket Layer virtual private network (SSL VPN) gateway and enter URL rewrite mode, use the **url rewrite** command in webvpn context configuration mode. To disable selected URL requests, use the **no** form of this command.

url rewrite

no url rewrite

Syntax Description

This command has no arguments or keywords.

Command Default

All requests are mangled.

Command Modes

Webvpn context configuration (config-webvpn-context)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Configuring the **url rewrite** command enters the url rewrite submode, in which selected IP addresses or hosts are defined for mangling.

Examples

The following example shows that selective URL mangling has been configured for IP address 10.1.1.0 255.255.0.0:

```
Router (config)# webvpn context
Router (config-webvpn-context)# url rewrite
Router (config-webvpn-url-rewrite)# ip 10.1.0.0 255.255.0.0
```

Related Commands

Command	Description
host (webvpn url rewrite)	Selects the name of the host site to be mangled on an SSL VPN gateway.
ip (webvpn url rewrite)	Configures the IP address of the site to be mangled on an SSL VPN gateway.
unmatched-action (webvpn url rewrite)	Defines the action when the user request does not match the IP address or host site configuration.

urlfilter

To enable Cisco IOS URL filtering, use the **urlfilter** command in policy-map-class configuration mode. To disable URL filtering, use the **no** form of this command.

urlfilter *parameter-map-name*

no urlfilter *parameter-map-name*

Syntax Description

parameter-map-name	Name of the parameter map for the URL filter.

Command Default

None

Command Modes

Policy-map-class configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use this command only after entering the **policy-map type inspect**, **class type inspect**, and **parameter-map type inspect** commands.

Examples

The following example enables Cisco IOS firewall URL filtering:

```
policy-map type inspect p1
 class type inspect c1
  urlfilter param1
```

Related Commands

Command	Description
class type inspect	Specifies the traffic (class) on which an action is to be performed.
policy-map type inspect	Creates Level 3 and Level 4 inspect type policy maps.

url-list

To enter webvpn URL list configuration mode to configure a list of URLs to which a user has access on the portal page of a Secure Sockets Layer Virtual Private Network (SSL VPN) and to attach the URL list to a policy group, use the **url-list** command in webvpn context configuration and webvpn group policy configuration mode, respectively. To remove the URL list from the SSL VPN context configuration and from the policy group, use the **no** form of this command.

url-list *name*

no url-list *name*

Syntax Description

name	Name of the URL list. The list name can up to 64 characters in length.

Command Default

Webvpn URL list configuration mode is not entered, and a list of URLs to which a user has access on the portal page of a SSL VPN website is not configured. If the command is not used to attach a URL list to a policy group, then a URL list is not attached to a group policy.

Command Modes

Webvpn context configuration
Webvpn group policy configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Entering this command places the router in SSL VPN URL list configuration mode. In this mode, the list of URLs is configured. A URL list can be configured under the SSL VPN context configuration and then separately for each individual policy group configuration. Individual URL list configurations must have unique names.

Examples

The following example creates a URL list:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# url-list ACCESS
Router(config-webvpn-url)# heading "Quick Links"
Router(config-webvpn-url)# url-text "Human Resources" url-value hr.mycompany.com
Router(config-webvpn-url)# url-text Engineering url-value eng.mycompany.com
Router(config-webvpn-url)# url-text "Sales and Marketing" products.mycompany.com
```

The following example attaches a URL list to a policy group configuration:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# url-list ACCESS
Router(config-webvpn-url)# heading "Quick Links"
Router(config-webvpn-url)# url-text "Human Resources" url-value hr.mycompany.com
Router(config-webvpn-url)# url-text Engineering url-value eng.mycompany.com
Router(config-webvpn-url)# url-text "Sales and Marketing" products.mycompany.com
Router(config-webvpn-url)# exit
```

```
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# url-list ACCESS
```

Related Commands

Command	Description
heading	Configures the heading that is displayed above URLs listed on the portal page of a SSL VPN website.
policy group	Attaches a URL list to policy group configuration.
url-list	Enters webvpn URL list configuration mode to configure the list of URLs to which a user has access on the portal page of a SSL VPN website.
url-text	Adds an entry to a URL list.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

url-profile

To specify a URL profile that configures the SDP registrar to run HTTPS, use the **url-profile** command in tti-registrar configuration mode. To remove this configuration, use the **no** form of this command.

url-profile {**start** *profile-name* | **intro** *profile-name*}

no url-profile {**start** *profile-name* | **intro** *profile-name*}

Syntax Description

start	Indicates that a URL profile is to be associated with the Start SDP deployment phase of iPhone deployment.
intro	indicate that a URL profile is to be associated with the Introduction SDP deployment phase of iPhone deployment.
profile-name	Specifies the name of a unique URL profile.

Command Default

No URL profile is defined for the iPhone deployment.

Command Modes

Tti-registrar configuration mode (tti-registrar)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The SDP Registrar is enabled to run HTTPs. It is recommended that the **ip http secure-server** command is issued to enable the HTTPS web server. If a secure server is enabled, then the **ip http secure-trustpoint** command should also be issued. Disable standard HTTP server through the **no ip http server** command (if the standard server is enabled). The specified trustpoint is a registrar local trustpoint appropriate for HTTPS communication between the registrar and the iPhone's browser.

The **url-profile** command can use the same or a different URL profile for the Introduction and Start SDP deployment phases.

Examples

The following example configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network from global configuration mode:

```
Router(config)# crypto provisioning registrar
Router(tti-registrar)# url-profile start START
Router(tti-registrar)# url-profile intro INTRO
Router(tti-registrar)# match url /sdp/intro
Router(tti-registrar)# match authentication trustpoint apple-tp
Router(tti-registrar)# match certificate cat 10
Router(tti-registrar)# mime-type application/x-apple-aspen-config
Router(tti-registrar)# template location flash:intro.mobileconfig
Router(tti-registrar)# template variable p iphone-vpn
```

Related Commands

Command	Description
crypto provisioning registrar	Configures a device to become a registrar for the SDP exchange and enters tti-registrar configuration mode.
match url	Specifies the URL to be associated with the URL profile.
match authentication trustpoint	Enters the trustpoint name that should be used to authenticate the peer's certificate.
match certificate	Enters the name of the certificate map used to authorize the peer's certificate.
mime-type	Specifies the MIME type that the SDP registrar should use to respond to a request received through the URL profile.
template location	Specifies the location of the template that the SDP Registrar should use while responding to a request received through the URL profile.
template variable p	Specifies the value that goes into the OU field of the subject name in the certificate to be issued.

url-text

To add an entry to a URL list, use the **url-text** command in webvpn URL list configuration mode. To remove the entry from a URL list, use the **no** form of this command.

url-text {*name* **url-value** *url*}

no url-text {*name* **url-value** *url*}

Syntax Description

name	Text label for the URL. The label must be inside quotation marks if it contains spaces.
url-value *url*	An HTTP URL.

Command Default

An entry is not added to a URL list.

Command Modes

Webvpn URL list configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

The following example configures a heading for a URL list:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# url-list ACCESS
Router(config-webvpn-url)# heading "Quick Links"
Router(config-webvpn-url)# url-text "Human Resources" url-value hr.mycompany.com
Router(config-webvpn-url)# url-text Engineering url-value eng.mycompany.com
Router(config-webvpn-url)# url-text "Sales and Marketing" products.mycompany.com
```

Related Commands

Command	Description
url-list	Enters webvpn URL list configuration mode to configure the list of URLs to which a user has access on the portal page of a SSL VPN website.

usage

To specify the intended use for the certificate, use the **usage** command in ca-trustpoint configuration mode. To restore the default behavior, use the **no** form of this command.

usage *method1* [*method2* [*method3*]]

no usage *method1* [*method2* [*method3*]]

Syntax Description

method1 [*method2* [*method3*]]	Intended use for the certificate; the available options are **ike**, **ssl-client**, and **ssl-server**. You must choose at least one method, and you may choose all three methods.

Defaults

ike

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Before you can issue the **usage** command, you must enable the **crypto ca trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.

This command may be used as a hint to set or clear key usage or other attributes in the certificate request.

Examples

The following example shows how to specify the certificate named "frog" for Internet Key Exchange (IKE):

```
crypto ca trustpoint frog
 enrollment url http://frog.phoobin.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet-0
 usage ike
 auto-enroll regenerate
 password revokeme
 rsa-key frog 2048
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

user

To enter the names of users that are allowed to authenticate using the local authentication server, use the **user** command in local RADIUS server configuration mode. To remove the username and password from the local RADIUS server, use the **no** form of this command.

user *username* {**password** | **nthash**} *password* [**group** *group-name* | **mac-auth-only**]

no user *username* {**password** | **nthash**} *password* [**group** *group-name* | **mac-auth-only**]

Syntax Description

username	Name of the user that is allowed to authenticate using the local authentication server.
password	Indicates that the user password will be entered.
nthash	Indicates that the NT value of the password will be entered.
password	User password.
group *group-name*	(Optional) Name of group to which the user will be added.
mac-auth-only	(Optional) Specifies that the user is allowed to authenticate using only MAC authentication.

Defaults

If no group name is entered, the user is not assigned to a VLAN and is never required to reauthenticate.

Command Modes

Local RADIUS server configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200.
12.2(15)JA	This command was modified to support MAC address authentication on the local authenticator.
12.3(2)JA	This command was modified to support EAP-FAST authentication on the local authenticator.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

This command is not supported on bridges.

If you do not know the user password, look up the NT value of the password in the authentication server database, and enter the NT hash as a hexadecimal string.

Examples

The following example shows that the user named “user1” has been allowed to authenticate using the local authentication server (using the password “userisok”). This user will be added to the group named “team1”.

```
Router(config-radsrv)# user user1 password userisok group team1
```

The following example shows how to add a user to the list of clients allowed to authenticate using MAC-based authentication on the local authenticator.

```
AP(config-radsrv)# user 00074218d01b password 00074218d01b group cashiers
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
vlan	Specifies a VLAN to be used by members of a user group.

user-group

To define a user group for dynamically authenticating and enforcing security policies on a per user basis, use the **user-group** command in identity policy configuration mode. To delete the user-group, use the **no** form of this command.

user-group *group-name*

no user-group *group-name*

Syntax Description

group-name	Name of the user-group.

Command Default

None

Command Modes

Identity policy configuration (config-identity policy)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The **user-group** command is used if the Tag and Template method of user-group support is used. The Tag and Template method associates IP addresses with user-groups using locally defined policies. A tag is received from the access control server (ACS), and this tag matches a template (identity policy with defined user-group) on the network access device (NAD).

To use the **user-group** command, you must first enter identity policy configuration mode by using the **identity policy** command. The identity policy defines one or more user-groups, to which source IP addresses are associated.

Note Another method of user-group association is available. User-group support can be achieved by configuring the supplicant-group attribute on the ACS.

Examples

The following example creates the identity policy “auth_proxy_ip” and configures the user-group “auth_proxy_ug”:

```
Router(config)# identity policy auth_proxy_ip
Router(config-identity-policy)# user-group auth_proxy_ug
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
identity policy	Creates an identity policy.

user-group logging

To enable user-group syslogs, use the **user-group logging** command in global configuration mode. To disable user-group syslogs, use the **no** form of this command.

user-group logging [**group** *group-name*]

no user-group logging [**group** *group-name*]

Syntax Description

group	(Optional) Configures logging for a specific user group.
group-name	(Optional) Name of the user-group.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example enables syslogs for the user-group “auth_proxy_ug”:

```
Router(config)# user-group logging group auth_proxy_ug
```

Related Commands

Command	Description
user-group	Creates a user-group for dynamically authenticating and enforcing security policies on a per user basis

username

To establish a username-based authentication system, use the **username** command in global configuration mode. To remove an established username-based authentication, use the **no** form of this command.

username *name* {**nopassword** | **password** *password* | **password** *encryption-type encrypted-password*}

username *name* **one-time** {**password** {**0** | **7** | *password*} | **secret** {**0** | **5** | *password*}}

username *name* **password** *secret*

username *name* [**access-class** *number*]

username *name* [**autocommand** *command*]

username *name* [**callback-dialstring** *telephone-number*]

username *name* [**callback-rotary** *rotary-group-number*]

username *name* [**callback-line** [**tty**] *line-number* [*ending-line-number*]]

username *name* **dnis**

username *name* [**nocallback-verify**]

username *name* [**noescape**]

username *name* [**nohangup**]

username one-time {**password** {**0** | **7** | *password*} | **secret** {**0** | **5** | *password*}}

username *name* [**privilege** *level*]

username *name* [**secret** {**0** | **5** | *password*}]

username *name* **user-maxlinks** *number*

username [**lawful-intercept**] *name* [**privilege** *privilege-level* | **view** *view-name*] **password** *password*

no username *name*

Syntax Description

name	Hostname, server name, user ID, or command name. The *name* argument can be only one word. Blank spaces and quotation marks are not allowed.
nopassword	No password is required for this user to log in. This is usually the most useful keyword to use in combination with the **autocommand** keyword.
password	Specifies a possibly encrypted password for a username.
password	Password that a user enters.

encryption-type	Single-digit number that defines whether the text immediately following is encrypted and if so, what type of encryption is used. Defined encryption types are 0, which means that the text immediately following is not encrypted, and 7, which means that the text is encrypted using a Cisco-defined encryption algorithm.
encrypted-password	Encrypted password that a user enters.
one-time	Specifies that the username and password is valid for only one time. This configuration is used to prevent default credentials from remaining in user configurations.
0	Specifies that an unencrypted password or secret (depending on the configuration) follows.
7	Specifies that a hidden password follows.
secret	Specifies a secret for the user.
5	Specifies that a hidden secret follows.
password	Specifies the password to access the *name* argument. A password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the **username** command.
secret	For Challenge Handshake Authentication Protocol (CHAP) authentication: specifies the secret for the local router or the remote device. The secret is encrypted when it is stored on the local router. The secret can consist of any string of up to 11 ASCII characters. There is no limit to the number of username and password combinations that can be specified, allowing any number of remote devices to be authenticated.
access-class	(Optional) Specifies an outgoing access list that overrides the access list specified in the **access-class** command available in line configuration mode. It is used for the duration of the user's session.
number	(Optional) Access list number.
autocommand	(Optional) Causes the specified command to be issued automatically after the user logs in. When the command is complete, the session is terminated. Because the command can be any length and can contain embedded spaces, commands using the **autocommand** keyword must be the last option on the line.
command	(Optional) The command string. Because the command can be any length and contain embedded spaces, commands using the **autocommand** keyword must be the last option on the line.
callback-dialstring	(Optional) For asynchronous callback only: permits you to specify a telephone number to pass to the DCE device.
telephone-number	(Optional) For asynchronous callback only: telephone number to pass to the DCE device.
callback-rotary	(Optional) For asynchronous callback only: permits you to specify a rotary group number. The next available line in the rotary group is selected.
rotary-group-number	(Optional) For asynchronous callback only: integer from 1 to 100 that identifies the group of lines on which you want to enable a specific username for callback.
callback-line	(Optional) For asynchronous callback only: specific line on which you enable a specific username for callback.
tty	(Optional) For asynchronous callback only: standard asynchronous line.

line-number	(Optional) For asynchronous callback only: relative number of the terminal line (or the first line in a contiguous group) on which you want to enable a specific username for callback. Numbering begins with zero.
ending-line-number	(Optional) Relative number of the last line in a contiguous group on which you want to enable a specific username for callback. If you omit the keyword (such as **tty**), then *line-number* and *ending-line-number* are absolute rather than relative line numbers.
dnis	Does not require a password when obtained via Dialed Number Identification Service (DNIS).
nocallback-verify	(Optional) Specifies that the authentication is not required for EXEC callback on the specified line.
noescape	(Optional) Prevents a user from using an escape character on the host to which that user is connected.
nohangup	(Optional) Prevents Cisco IOS software from disconnecting the user after an automatic command (set up with the **autocommand** keyword) has completed. Instead, the user gets another EXEC prompt.
privilege	(Optional) Sets the privilege level for the user.
level	(Optional) Number between 0 and 15 that specifies the privilege level for the user.
user-maxlinks	Limits the user's number of inbound links.
number	User-maxlinks limit for inbound links.
lawful-intercept	(Optional) Configures lawful intercept users on a Cisco device.
name	Hostname, server name, user ID, or command name. The *name* argument can be only one word. Blank spaces and quotation marks are not allowed.
privilege	(Optional) Sets the privilege level for the user.
privilege-level	(Optional) Number from 1 to 15 that specifies the privilege level for the user.
view	(Optional) For CLI view only: associates a CLI view name with the local authentication, authorization, and accounting (AAA) database.
view-name	(Optional) For CLI view only: view name, which is specified via the **parser view** command, that is to be associated with the AAA local database.
password *password*	Password to access the CLI view.

Command Default No username-based authentication system is established.

Command Modes Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
11.1	This command was modified. The following keywords and arguments were added: • **callback-dialstring** *telephone-number* • **callback-rotary** *rotary-group-number* • **callback-line** [**tty**] *line-number* [*ending-line-number*] • **nocallback-verify**
12.3(7)T	This command was modified. The following keywords and arguments were added: • **lawful-intercept** • **view** • *view-name*
12.2(33)SRB	This command was modified. The following keywords and arguments were integrated into Cisco IOS Release 12.2(33)SRB: • **lawful-intercept** • **view** • *view-name*
12.2(33)SB	This command was modified. The following keywords and arguments were integrated into Cisco IOS Release 12.2(33)SB: • **lawful-intercept** • **view** • *view-name*
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.4	This command was modified. The following keywords were integrated into Cisco IOS Release 12.4: • **one-time** • **secret** • **0, 5, 7**
15.1(1)S	This command was modified. Support for the **nohangup** keyword was removed from Secure Shell (SSH).

Usage Guidelines

The **username** command provides username or password authentication, or both, for login purposes only.

Multiple **username** commands can be used to specify options for a single user.

Add a username entry for each remote system with which the local router communicates and from which it requires authentication. The remote device must have a username entry for the local router. This entry must have the same password as the local router's entry for that remote device.

This command can be useful for defining usernames that get special treatment. For example, you can use this command to define an "info" username that does not require a password but connects the user to a general purpose information service.

The **username** command is required as part of the configuration for CHAP. Add a username entry for each remote system from which the local router requires authentication.

Note

- To enable the local router to respond to remote CHAP challenges, one **username** *name* entry must be the same as the **hostname** entry that has already been assigned to the other router.
- To avoid the situation of a privilege level 1 user entering into a higher privilege level, configure a per-user privilege level other than 1 (for example, 0 or 2 through 15).
- Per-user privilege levels override virtual terminal privilege levels.

In Cisco IOS Release 15.1(1)S and later releases, the **nohangup** keyword is not supported with SSH. If the **username** *user* **autocommand** *command-name* command is configured and SSH is used, the session disconnects after executing the configured command once. This behavior with SSH is opposite to the Telnet behavior, where Telnet continuously asks for authentication and keeps executing the command until the user exits Telnet manually.

CLI and Lawful Intercept Views

Both CLI views and lawful intercept views restrict access to specified commands and configuration information. A lawful intercept view allows a user to secure access to lawful intercept commands that are held within the TAP-MIB, which is a special set of Simple Network Management Protocol (SNMP) commands that stores information about calls and users.

Users who are specified via the **lawful-intercept** keyword are placed in the lawful-intercept view, by default, if no other privilege level or view name has been explicitly specified.

If no value is specified for the *secret* argument and the **debug serial-interface** command is enabled, an error is displayed when a link is established and the CHAP challenge is not implemented. The CHAP debugging information is available using the **debug ppp negotiation**, **debug serial-interface**, and **debug serial-packet** commands. For more information about **debug** commands, refer to the *Cisco IOS Debug Command Reference*.

Examples

The following example shows how to implement a service similar to the UNIX **who** command, which can be entered at the login prompt and lists the current users of the router:

```
username who nopassword nohangup autocommand show users
```

The following example shows how to implement an information service that does not require a password to be used. The command takes the following form:

```
username info nopassword noescape autocommand telnet nic.ddn.mil
```

The following example shows how to implement an ID that works even if all the TACACS+ servers break. The command takes the following form:

```
username superuser password superpassword
```

The following example shows how to enable CHAP on interface serial 0 of "server_l." It also defines a password for a remote server named "server_r."

```
hostname server_1
username server_r password theirsystem
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

The following is output from the **show running-config** command displaying the passwords that are encrypted:

```
hostname server_1
username server_r password 7 121F0A18
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

In the following example, a privilege level 1 user is denied access to privilege levels higher than 1:

```
username user privilege 0 password 0 cisco
username user2 privilege 2 password 0 cisco
```

The following example shows how to remove the username-based authentication for user2:

```
no username user2
```

Related Commands

Command	Description
arap callback	Enables an ARA client to request a callback from an ARA client.
callback forced-wait	Forces the Cisco IOS software to wait before initiating a callback to a requesting client.
debug ppp negotiation	Displays PPP packets sent during PPP startup, where PPP options are negotiated.
debug serial-interface	Displays information about a serial connection failure.
debug serial-packet	Displays more detailed serial interface debugging information than you can obtain using **debug serial interface** command.
ppp callback (DDR)	Enables a dialer interface that is not a DTR interface to function either as a callback client that requests callback or as a callback server that accepts callback requests.
ppp callback (PPP client)	Enables a PPP client to dial into an asynchronous interface and request a callback.
show users	Displays information about the active lines on the router.

username (dot1x credentials)

To specify the username for an 802.1X credentials profile, use the **username** command in dot1x credentials configuration mode. To remove the username, use the **no** form of this command.

username *name*

no username

Syntax Description

name	Name of the credentials profile.

Command Default

A username is not specified.

Command Modes

Dot1x credentials configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Before using this command, the **dot1x credentials** command must have been configured.

Examples

The following example shows which credentials profile should be used when configuring a supplicant:

```
dot1x credentials basic-user
 username router
 password secret
 description This credentials profile should be used for most configured ports
```

The credentials structure can be applied to an interface, along with the **dot1x pae supplicant** command and keyword, to enable supplicant functionality on that interface.

```
interface fastethernet 0/1
 dot1x credentials basic-user
 dot1x pae supplicant
```

Related Commands

Command	Description
dot1x credentials	Specifies an 802.1X credentials profile to be used.

username (ips-autoupdate)

To define a username and password in which to access signature files from the server, use the **username** command in IPS-auto-update configuration mode.

username *name* **password** *password*

Syntax Description

name	Username required to access the latest updated signature file package.
password *password*	Password required to access the latest updated signature file package.

Command Default

The default value is defined in the signature definition XML.

Command Modes

IPS-auto-update configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Automatic signature updates allow users to override the existing Intrusion Prevention System (IPS) configuration and automatically keep signatures up to date on the basis of a preset time, which can be configured to a preferred setting.

Use the **ip ips auto-update** command to enable Cisco IOS IPS to automatically update the signature file on the system. Thereafter, you can optionally issue the **username** command to specify a username and password to access signature files.

Examples

The following example shows how to configure automatic signature updates and issue the **show ip ips auto-update** command to verify the configuration:

```
Router# clock set ?
    hh:mm:ss Current Time
Router# clock set 10:38:00 20 apr 2006
Router#
*Apr 20 17:38:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 10:37:55 MST
Thu Apr 20 2006 to 10:38:00 MST Thu Apr 20 2006, configured from console by cisco on
console.

Router(config)# ip ips auto-update
Router(config-ips-auto-update)# occur-at 0 0-23 1-31 1-5
Router(config-ips-auto-update)# $s-auto-update/IOS_reqSeq-dw.xml
Router(config-ips-auto-update)#^Z
Router#
*May 4 2006 15:50:28 MST: IPS Auto Update: setting update timer for next update: 0 hrs 10
min
*May 4 2006 15:50:28 MST: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router#
Router# show ip ips auto-update
```

```
IPS Auto Update Configuration
    URL : tftp://192.168.0.2/jdoe/ips-auto-update/IOS_reqSeq-dw.xml
    Username : not configured
    Password : not configured
    Auto Update Intervals
      minutes (0-59) : 0
      hours (0-23) : 0-23
      days of month (1-31) : 1-31
      days of week: (0-6) : 1-5
```

Related Commands

Command	Description
ip ips auto-update	Enables automatic signature updates for Cisco IOS IPS.

username secret

To encrypt a user password with irreversible encryption, use the **username secret** command in global configuration mode.

username *name* **secret** {**0** *password* | **5** *secret-string* | **4** *secret-string*}

Syntax Description

name	Username.
0	Specifies an unencrypted secret.
password	Clear-text password.
5 *secret-string*	message digest alogrithm5 (MD5) encrypted secret text string, which is stored as the encrypted user password.
4 *secret-string*	SHA256 encrypted secret text string, which is stored as the encrypted user password.

Defaults

No username-based authentication system is established.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(18)S	This command was introduced.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S. Encryption types **0**, **4**, and **5** were added.

Usage Guidelines

Use the **username secret** command to configure a username and MD5-encrypted user password. MD5 encryption is a strong encryption method that is not retrievable; thus, you cannot use MD5 encryption with protocols that require clear-text passwords, such as Challenge Handshake Authentication Protocol (CHAP).

The **username secret** command provides an additional layer of security over the username password. It also provides better security by encrypting the password using non reversible MD5 encryption and storing the encrypted text. The added layer of MD5 encryption is useful in environments in which the password crosses the network or is stored on a TFTP server.

Use MD5 as the encryption type if you paste into this command an encrypted password that you copied from a router configuration file.

Use this command to enable Enhanced Password Security for the specified, unretrievable username. This command enables MD5 encryption on the password. MD5 encryption is a strong encryption method. You cannot use MD5 encryption with protocols, such as CHAP, that require clear-text passwords.

This command can be useful for defining usernames that get special treatment. For example, you can use this command to define an "info" username that does not require a password but connects the user to a general-purpose information service.

The **username** command provides username or secret authentication for login purposes only. The *name* argument can be one word only. Spaces and quotation marks are not allowed. You can use multiple **username** commands to specify options for a single user.

Examples

The following example shows how to configure username "abc" and enable MD5 encryption on the clear-text password "xyz":

```
username abc secret 0 xyz
```

The following example shows how to configure username "cde" and enter an MD5 encrypted text string that is stored as the username password:

```
username cde secret 5 $1$feb0$a104Qd9UZ./Ak00KTggPD0
```

The following example shows how to configure username "xyz" and enter an MD5 encrypted text string that is stored as the username password:

```
username xyz secret 5 $1$feb0$a104Qd9UZ./Ak00KTggPD0
```

Related CommandsL

Command	Description
enable password	Sets a local password to control access to various privilege levels.
enable secret	Specifies an additional layer of security over the enable password command.
username	Establishes a username-based authentication system.

user-profile location

To store user bookmarks in a directory on a device, use the **user-profile location** command in webvpn context configuration mode. To remove a directory that has been configured, use the **no** form of this command.

user-profile location device:*directory*

no user-profile location device:*directory*

Syntax Description

device:	Storage location on a device. See Table 222 for a list of acceptable storage locations.
directory	Name of the directory.

Command Default

The default location is flash:/webvpn/<context-name>/.

Command Modes

Webvpn context configuration (config-webvpn-context)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Table 222 lists accept storage locations.

Table 222 Type of Storage Location

Type of Storage Location	Description
archive	Archived file system.
Bootflash	Bootflash memory.
disk0	On Disk 0.
disk1	On Disk 1.
Flash	Flash memory.
FTP	FTP network server.
HTTP	HTTP file server.
HTTPS	HTTP secure server.
null	Null destination for copies. You can copy a remote file to null to determine its size.
NVRAM	Storage location is in NVRAM.
PRAM	Phase-change memory (PRAM)—type of nonvolatile computer memory.

Table 222 Type of Storage Location (continued)

Type of Storage Location	Description
RCP	Remote copy protocol network server.
SCP	Secure Copy—A means of securely transferring computer files between a local and a remote host or between two remote hosts using the Secure Shell (SSH) protocol.
slot0	On Slot 0.
slot1	On Slot 1.
system	System memory, including the running configuration.
tmpsys	Temporary system in a file system.

Examples

The following example shows bookmarks are stored in flash on the directory webvpn/sslvpn_context/.

```
Router# webvpn context context1
Router# user-profile location flash:/webvpn/sslvpn_context/
```

Related Commands

Command	Description
webvpn context	Configures the SSL VPN context and enters webvpn context configuration mode.

view

To add a normal command-line interface (CLI) view to a superview, use the **view** command in view configuration mode. To remove a CLI view from a superview, use the **no** form of this command.

view *view-name*

no view *view-name*

Syntax Description

view-name	CLI view that is to be added to the given superview.

Defaults

A superview will not contain any CLI views until this command is enabled.

Command Modes

View configuration (config-view)

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IO XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Before you can use this command to add normal views to a superview, ensure that the following steps have been taken:

- A password has been configured for the superview (via the **secret 5** command).
- The normal views that are to be added to the superview are valid views in the system; that is, the views have been successfully created via the **parser view** command.

Examples

The following sample output from the **show running-config** command shows that “view_one” and “view_two” have been added to superview “su_view1,” and “view_three” and “view_four” have been added to superview “su_view2”:

```
!
parser view su_view1 superview
 secret 5 <encoded password>
 view view_one
 view view_two
!
parser view su_view2 superview
 secret 5 <encoded password>
 view view_three
 view view_four
!
```

Related Commands

Command	Description
parser view	Creates or changes a CLI view and enters view configuration mode.
secret 5	Associates a CLI view or a superview with a password.

virtual-template (IKEv2 profile)

To configure an Internet Key Exchange (IKEv2) profile with a virtual template to be used for cloning the virtual access interfaces, use the **virtual-template** command in IKEv2 profile configuration mode. To remove the virtual template from IKEv2 profile, use the **no** form of this command.

virtual-template *template-number*

no virtual-template *template-number*

Syntax Description

template-number	Identifying number of the virtual template that will be used to clone virtual access interfaces.

Command Default

A virtual template is not specified.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to specify the virtual template for cloning a virtual access interface.

Examples

The following example shows the configuration of two IKEv2 profiles:

```
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# virtual-template 1
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.
show ikev2 profile	Displays the default or user-defined IKEv2 profile.

virtual-template (webvpn context)

To associate a virtual template with a Secure Socket Layer Virtual Private Network (SSL VPN) context, use the **virtual-template** command in webvpn context configuration mode. To disable the configuration, use the **no** form of this command.

virtual-template *template-number* [**tunnel**]

no virtual-template

Syntax Description

template-number	Number of the virtual template that will be used to clone virtual access interfaces. The range is from 1 to 1000.
tunnel	(Optional) Applies the virtual template for every full tunnel session.

Command Default

No virtual template is enabled.

Command Modes

Webvpn context configuration (config-webvpn-context)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.1(1)T	This command was modified. The **tunnel** keyword was added.

Usage Guidelines

You can configure the desired IP features in the virtual template and then use the **virtual-template** command to apply the configuration on a per-context or per-tunnel basis. The per-context configuration applies the IP features to all the users connecting to that WebVPN context and the per-tunnel configuration applies the IP features for each SSL VPN full tunnel established in the WebVPN context.

Examples

The following example shows how to associate a virtual template with an SSL VPN context:

```
Router# configure terminal
Router(config)# webvpn context context1
Router(config-webvpn-context)# virtual-template 1
```

Related Commands

Command	Description
inservice	Enables an SSL VPN context.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

vlan (local RADIUS server group)

To specify a VLAN to be used by members of the user group, use the **vlan** command in local RADIUS server group configuration mode. To reset the parameter to the default value, use the **no** form of this command.

vlan *vlan*

no vlan *vlan*

Syntax Description

vlan	VLAN ID.

Defaults

No default behavior or values

Command Modes

Local RADIUS server group configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

The access point or router moves group members into the VLAN that you specify, overriding any other VLAN assignments. You can assign only one VLAN to a user group.

Examples

The following example shows that VLAN “225” is to be used by members of the user group:

```
vlan 225
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.

Command	Description
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.

vlan group

To create or modify a VLAN group, use the **vlan group** command in global configuration mode. To remove a VLAN list from the VLAN group, use the **no** form of this command.

vlan group *group-name* **vlan-list** *vlan-list*

no vlan group *group-name* **vlan-list** *vlan-list*

Syntax Description

group-name	VLAN group name.
vlan-list	VLAN list name. See the "Usage Guidelines" section for additional information about the *vlan-list* argument.

Defaults

This command has no default settings.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXI1	This command was introduced.

Usage Guidelines

The VLAN group name may contain up to 32 characters and must begin with a letter.

The *vlan-list* argument can be a single VLAN ID, a list of VLAN IDs, or VLAN ID ranges (*vlan-id-vlan-id*). Multiple entries are separated by a hyphen (-) or a comma (,).

If the named VLAN group does not exist, the **vlan group** command creates the group and maps the specified VLAN list to the group. If the named VLAN group exists, the specified VLAN list is mapped to the group.

The **no** form of the **vlan group** command removes the specified VLAN list from the VLAN group. When you remove the last VLAN from the VLAN group, the VLAN group is deleted.

A maximum of 100 VLAN groups can be configured, and a maximum of 4094 VLANs can be mapped to a VLAN group.

Examples

This example shows how to map VLANs 7 through 9 and 11 to a VLAN group:

```
Router(config)# vlan group ganymede vlan-list 7-9,11
```

This example shows how to remove VLAN 7 from the VLAN group:

```
Router(config)# no vlan group ganymede vlan-list 7
```

Related Commands

Command	Description
show vlan group	Displays the VLANs mapped to VLAN groups.

vpdn aaa attribute

To enable reporting of network access server (NAS) authentication, authorization, and accounting (AAA) attributes related to a virtual private dialup network (VPDN) to the AAA server, use the **vpdn aaa attribute** command in global configuration mode. To disable reporting of AAA attributes related to VPDN, use the **no** form of this command.

vpdn aaa attribute {**nas-ip-address vpdn-nas** | **nas-port** {**vpdn-nas** | **physical-channel-id**}}

no vpdn aaa attribute {**nas-ip-address vpdn-nas** | **nas-port**}

Syntax Description

nas-ip-address vpdn-nas	Enables reporting of the VPDN NAS IP address to the AAA server.
nas-port vpdn-nas	Enables reporting of the VPDN NAS port to the AAA server.
nas-port physical-channel-id	Enables reporting of the VPDN NAS port physical channel identifier to the AAA server.

Command Default

AAA attributes are not reported to the AAA server.

Command Modes

Global configuration

Command History

Release	Modification
11.3NA	This command was introduced.
11.3(8.1)T	This command was integrated into Cisco IOS Release 11.3(8.1)T.
12.1(5)T	This command was modified to support the PPP extended NAS-Port format.
12.2(13)T	Support was added for the **physical-channel-id** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command can be used with RADIUS or TACACS+, and is applicable only on the VPDN tunnel server.

The PPP extended NAS-Port format enables the NAS-Port and NAS-Port-Type attributes to provide port details to a RADIUS server when one of the following protocols is configured:

- PPP over ATM
- PPP over Ethernet (PPPoE) over ATM
- PPPoE over 802.1Q VLANs

Before PPP extended NAS-Port format attributes can be reported to the RADIUS server, the **radius-server attribute nas-port format** command with the **d** keyword must be configured on both the tunnel server and the NAS, and the tunnel server and the NAS must both be Cisco routers.

Note Reporting of NAS AAA attributes related to a VPDN on a AAA server is not supported for Point-to-Point Tunneling Protocol (PPTP) sessions with multihop deployment.

Examples

The following example configures VPDN on a tunnel server and enables reporting of VPDN AAA attributes to the AAA server:

```
vpdn enable
vpdn-group 1
 accept-dialin
  protocol any
  virtual-template 1
!
 terminate-from hostname nas1
 local name ts1
!
vpdn aaa attribute nas-ip-address vpdn-nas
vpdn aaa attribute nas-port vpdn-nas
vpdn aaa attribute nas-port physical-channel-id
```

The following example configures the tunnel server for VPDN, enables AAA, configures a RADIUS AAA server, and enables reporting of PPP extended NAS-Port format values to the RADIUS server. PPP extended NAS-Port format must also be configured on the NAS for this configuration to be effective.

```
vpdn enable
vpdn-group L2TP-tunnel
 accept-dialin
  protocol l2tp
  virtual-template 1
!
 terminate-from hostname nas1
 local name ts1
!
aaa new-model
aaa authentication ppp default local group radius
aaa authorization network default local group radius
aaa accounting network default start-stop group radius
!
radius-server host 172.16.79.76 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute nas-port format d
radius-server key ts123
!
vpdn aaa attribute nas-port vpdn-nas
```

Related Commands

Command	Description
radius-server attribute nas-port format	Selects the NAS-Port format used for RADIUS accounting features.

vrf (isakmp profile)

To define the virtual routing and forwarding (VRF) value to which the IP Security (IPSec) tunnel will be mapped, use the **vrf** command in Internet Security Association Key Management (ISAKMP) profile configuration mode. To disable the VRF that was defined, use the **no** form of this command.

vrf *ivrf*

no vrf *ivrf*

Syntax Description

ivrf	VRF to which the IPSec tunnel will be mapped.

Defaults

The VRF will be the same as the front door VRF (FVRF).

Command Modes

ISAKMP profile configuration (config-isa-prof)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Use this command to map IPSec tunnels that terminate on a global interface to a specific Virtual Private Network (VPN).

If traffic from the router to a certification authority (CA) (for authentication, enrollment, or for obtaining a certificate revocation list [CRL]) or to a Lightweight Directory Access Protocol (LDAP) server (for obtaining a CRL) needs to be routed via a VRF, the **vrf** command must be added to the trustpoint. Otherwise, such traffic will use the default routing table.

If a profile does not specify one or more trustpoints, all trustpoints in the router will be used to attempt to validate the certificate of the peer (Internet Key Exchange [IKE] main mode or signature authentication). If one or more trustpoints are specified, only those trustpoints will be used.

Examples

The following example shows that two IPSec tunnels to VPN 1 and VPN 2 are terminated:

```
crypto isakmp profile vpn1
 vrf vpn1
 keyring vpn1
 match identity address 172.16.1.1 255.255.255.255
crypto isakmp profile vpn2
 vrf vpn2
 keyring vpn2
 match identity address 10.1.1.1 255.255.255.255
```

```
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
crypto ipsec transform-set vpn2 esp-3des esp-md5-hmac
!
crypto map crypmap 1 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set vpn1
 set isakmp-profile vpn1
 match address 101
crypto map crypmap 3 ipsec-isakmp
 set peer 10.1.1.1
 set transform-set vpn2
 set isakmp-profile vpn2
 match address 102
!
!
interface Ethernet1/2
 ip address 172.26.1.1 255.255.255.0
 duplex half
 no keepalive
 no cdp enable
 crypto map crypmap
```

vrfname

To associate a Virtual Private Network (VPN) front-door routing and forwarding instance (FVRF) with a SSL VPN gateway, use the **vrfname** command in webvpn gateway configuration mode. To disassociate the FVRF from the SSL VPN gateway, use the **no** form of this command.

vrfname *name*

no vrfname *name*

Syntax Description

name	Name of the VRF.

Command Default

A VPN FVRF is not associated with a SSL VPN gateway.

Command Modes

Webvpn gateway (config-webvpn-gateway)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Only one FVRF can be associated with each SSL VPN context configuration.

Examples

The following example shows FVRF has been configured:

```
Router (config) ip vrf vrf_1
Router (config-vrf) end
Router (config) webvpn gateway mygateway
Router (config-webvpn-gateway) vrfname vrf_1
Router (cofig-webvpn-gateway) end
```

Related Commands

Command	Description
webvpn gateway	Enters webvpn gateway configuration mode to configure a SSL VPN gateway.

vrf-name

To associate a Virtual Private Network (VPN) routing and forwarding instance (VRF) with a SSL VPN context, use the **vrf-name** command in webvpn context configuration mode. To remove the VRF from the WebVPN context configuration, use the **no** form of this command.

vrf-name *name*

no vrf-name

Syntax Description

name	Name of the VRF.

Command Default

A VPN VRF is not associated with a SSL VPN context.

Command Modes

Webvpn context configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The VRF is first defined in global configuration mode. Only one VRF can be associated with each SSL VPN context configuration.

Examples

The following example associates a VRF with a SSL VPN context:

```
Router (config)# ip vrf BLUE
Router (config-vrf)# rd 10.100.100.1
Router (config-vrf)# webvpn context context1
Router (config-webvpn-context)# vrf-name BLUE
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

web-agent-url

To configure the Netegrity agent URL to which Single SignOn (SSO) authentication requests will be dispatched, use the **web-agent-url** command in webvpn sso server configuration mode. To remove the Netegrity agent URL, use the **no** form of this command.

web-agent-url *url*

no web-agent-url *url*

Syntax Description

url	URL to which SSO authentication requests will be dispatched.

Command Default

Authentication requests will not be dispatched to a Netegrity agent URL.

Command Modes

Webvpn sso server configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Note A web agent URL and policy server secret key are required for a SSO server configuration. If they are not configured, a warning message is displayed. (See the warning message information in the Examples section below.)

Examples

The following example shows that SSO authentication requests will be dispatched to the URL http://www.example.com/webvpn/:

```
webvpn context context1
 sso-server test-sso-server
  web-agent-url http://www.example.com/webvpn/
```

Warning Message

If a web agent URL and policy server secret key are not configured, a message similar to the following is received:

```
Warning: must configure web agent URL for sso-server "example"
Warning: must configure SSO policy server secret key for sso-server "example"
Warning: invalid configuration. SSO for "example" being disabled
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

webvpn

Note Effective with Cisco IOS Release 12.4(6)T, the **webvpn** command is replaced by the **webvpn context** and **webvpn gateway** commands. See the these commands for more information.

To enter Web VPN configuration mode, use the **webvpn** command in global configuration mode. To remove all commands that were entered in Web VPN configuration mode, use the **no** form of this command.

webvpn

no webvpn

Syntax Description

This command has no arguments or keywords.

Defaults

Web VPN configuration mode is not entered.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(6)T	This command was replaced by the **webvpn context** and **webvpn gateway** commands.

Examples

The following example shows that Web VPN configuration mode has been entered:

```
Router (config)# webvpn
Router (config-webvpn)#
```

Related Commands

Command	Description
webvpn enable	Enables WebVPN in the system.

webvpn-homepage

To specify the WebVPN home page URL, use the **webvpn-homepage** command in WebVPN group policy configuration mode. To disable the configuration, use the **no** form of this command.

webvpn-homepage *homepage-url* [**redirection-time** *seconds*]

no webvpn-homepage

Syntax Description

homepage-url	Home page URL.
redirection-time *seconds*	(Optional) Specifies the home page redirection time, in seconds. The range is from 0 to 15. The default value is 5.

Command Default

The default reditection time is 5 seconds.

Command Modes

WebVPN group policy configuration (config-webvpn-group)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

You can use the **webvpn-homepage** command to specify the WebVPN home page URL and apply the WebVPN redirection time to a particular policy group users. This command helps you to customize and have your own portal page.

The portal page is not displayed if you configure the **webvpn-homepage** command and set the redirection time to 0. If the redirection time is greater than 0, then the portal page is displayed for the time the redirection time is configured and then redirects you to the home page.

If the configuration is not successful, an appropriate error message is displayed.

Examples

The following example shows how to specify the home page URL “http://192.0.2.0” with the redirection time of 12 seconds:

```
Router# configure terminal
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group policy1
Router(config-webvpn-group)# webvpn-homepage http://192.0.2.0 redirection-time 12
```

Related Commands

Command	Description
policy group	Enters WebVPN group policy configuration mode.
show webvpn policy group	Displays the context configuration associated with a policy group.
webvpn context	Enters WebVPN context configuration mode.

webvpn cef

To enable Secure Socket Layer virtual private network (SSL VPN) full-tunnel Cisco Express Forwarding (CEF) support, use the **webvpn cef** command in global configuration mode. To disable full-tunnel CEF support, use the **no** form of this command.

webvpn cef

no webvpn cef

Syntax Description

There are no arguments or keywords.

Command Default

This command is set by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

IP CEF must be turned on before this command can take effect.

Examples

The following example shows that full-tunnel CEF is being disabled:

```
Router (config)# no webvpn cef
```

Related Commands

Command	Description
ip cef	Enables CEF on the route processor card.

webvpn context

To enter webvpn context configuration mode to configure the Secure Sockets Layer Virtual Private Network (SSL VPN) context, use the **webvpn context** command in global configuration mode. To remove the SSL VPN configuration from the router configuration file, use the **no** form of this command.

webvpn context *name*

no webvpn context *name*

Syntax Description

name	Name of the SSL VPN context configuration.

Command Default

Webvpn context configuration mode is not entered, and a SSL VPN context is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The SSL VPN context defines the central configuration of the SSL VPN. Entering the **webvpn context** command places the router in webvpn context configuration mode.

Note The **ssl authenticate verify all** command is enabled by default when a context configuration is created. The context cannot be removed from the router configuration while a SSL VPN gateway is in an enabled state (in service).

Examples

The following example configures and activates the SSL VPN context configuration:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# inservice
```

Related Commands

Command	Description
aaa authentication (WebVPN)	Configures AAA authentication for SSL VPN sessions.
csd enable	Enables CSD support for SSL VPN sessions.
default-group-policy	Specifies a default group policy for SSL VPN sessions.
gateway (WebVPN)	Specifies the gateway for SSL VPN sessions.
inservice	Enables a SSL VPN gateway or context process.
login-message	Configures a message for a user login text box on the login page.

Command	Description
logo	Configures a custom logo to be displayed on the login and portal pages of a SSL VPN website.
max-users (WebVPN)	Limits the number of connections to a SSL VPN that will be permitted
nbns-list	Enters webvpn NBNS list configuration mode to configure a NBNS server list for CIFS name resolution.
policy group	Enters a webvpn group policy configuration mode to configure a group policy.
port-forward	Enters webvpn port-forward list configuration mode to configure a port-forwarding list.
secondary-color	Configures the color of the secondary title bars on the login and portal pages of a SSL VPN website.
secondary-text-color	Configures the color of the text on the secondary bars of a SSL VPN website.
title	Configures the HTML title string that is shown in the browser title and on the title bar of a SSL VPN website.
title-color	Configures the color of the title bars on the login and portal pages of a SSL VPN website.
url-list	Enters webvpn URL list configuration mode to configure the list of URLs to which a user has access on the portal page of a SSL VPN website.
vrf-name	Associates a VRF with a SSL VPN context.

webvpn create template

To create templates for multilanguage support for messages initiated by the head-end in a Secure Socket Layer Virtual Private Network (SSL VPN), configure the **webvpn create template** command in user EXEC or privileged EXEC mode.

webvpn create template {**browser-attribute** | **language** | **url-list**} *device***:**

Syntax Description

browser-attribute	Creates a template file named “battr_tpl.xml”.
language	Creates a template file named “lang.js”.
url-list	Creates a template file named “url_list_tpl.xml”.
*device***:**	Storage device on the system for the templates, such as flash: or disk0.

Command Default

Template files are not created.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

After template files have been created, they can be copied to a PC for editing and then reimported to the storage device.

Examples

The following example shows that a browser-attribute template file is to be created in flash:

```
Router# webvpn create template browser-attribute flash:
```

The following example shows that the language file is to be created in flash:

```
Router# webvpn create template language flash:
```

The following example shows that a URL list template is to be created in flash:

```
Router# webvpn create template url-list flash:
```

Related Commands

Command	Description
browser-attribute import	Imports user-defined browser attributes into a webvpn context.
import	Imports a user-defined URL list into a webvpn context.

Command	Description
language	Specifies the language to be used in a webvpn context.
url-list	Enters webvpn URL list configuration mode to configure a list of URLs to which a user has access on the portal page of a SSL VPN and attaches the URL list to a policy group.

webvpn enable

Note Effective with Cisco IOS Release 12.4(6)T, the **webvpn enable** command is replaced by the **inservice** command. See the **inservice** command for more information.

To enable WebVPN in the system, use the **webvpn enable** command in global configuration mode. To disable WebVPN in the system, use the **no** form of this command.

webvpn enable [**gateway-addr** *ip-address*]

no webvpn enable [**gateway-addr** *ip-address*]

Syntax Description

gateway-addr *ip-address*	(Optional) Enables WebVPN on only the IP address that is specified. If this keyword and argument are not configured, WebVPN is enabled globally on all IP addresses.

Defaults

WebVPN is disabled in the system.

Command Modes

Web VPN configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(6)T	This command was replaced by the **inservice** command.

Usage Guidelines

This command initializes the required system data structures, initializes TCP sockets, and performs other startup tasks related to WebVPN.

Examples

The following example shows that WebVPN has been enabled in the system:

```
webvpn enable
```

Related Commands

Command	Description
webvpn	Enters Web VPN configuration mode.

webvpn gateway

To enter webvpn gateway configuration mode to configure a SSL VPN gateway, use the **webvpn gateway** command in global configuration mode. To remove the SSL VPN gateway from the router configuration file, use the **no** form of this command.

webvpn gateway *name*

no webvpn gateway *name*

Syntax Description

name	Name of the virtual gateway service.

Command Default

Webvpn gateway configuration mode is not entered, and a SSL VPN gateway is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Entering the **webvpn gateway** command places the router in webvpn gateway configuration mode. Configuration settings specific to the SSL VPN gateway are entered in this configuration mode.

The SSL VPN gateway acts as a proxy for connections to protected resources. Protected resources are accessed through a secure encrypted connection between the gateway and a web-enabled browser on a remote device, such as a personal computer.

The gateway is configured using an IP address at which SSL VPN remote-user sessions terminate. The gateway is not active until the inservice command has been entered in SSL VPN gateway configuration mode. Only one gateway can be configured in a SSL VPN-enabled network.

Examples

The following example creates and enables a SSL VPN gateway process named SSL_GATEWAY:

```
Router(config)# webvpn gateway SSL_GATEWAY
Router(config-webvpn-gateway)# ip address 10.1.1.1 port 443
Router(config-webvpn-gateway)# ssl trustpoint SSLVPN
Router(config-webvpn-gateway)# http-redirect 80
Router(config-webvpn-gateway)# inservice
```

Related Commands

Command	Description
hostname (WebVPN)	Configures a SSL VPN hostname.
http-redirect	Configures HTTP traffic to be carried over HTTPS.
inservice	Enables a SSL VPN gateway or context process.
ip address (WebVPN)	Configures a proxy IP address on a SSL VPN gateway.

Command	Description
ssl encryption	Configures the specify the encryption algorithms that the SSL protocol will use for an SSL VPN.
ssl trustpoint	Configures the certificate trust point on a SSL VPN gateway.

webvpn import svc profile

To enable an AnyConnect profile to be imported from a router, use the **webvpn import svc profile** command in global configuration mode. To disable the configuration, use the **no** form of this command.

webvpn import svc profile *profile-name device-name*

no webvpn import svc profile *profile-name*

Syntax Description

profile-name	Name of the AnyConnect profile.
device-name	Device name and filename of the AnyConnect profile thats needs to be imported.

Command Default

AnyConnect profiles are not imported to the Cisco IOS headend.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

You can use the **webvpn import svc profile** command to import the AnyConnect profile to the Cisco IOS headend. In order to import the AnyConnect profile to the Cisco IOS headend, the administrator must download the AnyConnect profile from an AnyConnect client (this profile comes by default with AnyConnect), update the profile file to enable the AnyConnect support, and then import the modified profile into the Cisco IOS software.

Examples

The following example shows how to import the AnyConnect profile to the Cisco IOS headend:

```
Router> enable
Router# configure terminal
Router(config)# webvpn import svc profile profile1 disk0:filename
```

Related Commands

Command	Description
svc profile	Applies a particular AnyConnect profile to the webvpn gateway.

webvpn install

To install a Cisco Secure Desktop (CSD) or Cisco AnyConnect VPN Client package file to a Secure Socket Layer virtual private network (SSL VPN) gateway for distribution to end users, use the **webvpn install** command in global configuration mode. To remove a package file from the SSL VPN gateway, use the **no** form of this command.

webvpn install [**csd** *location-name* | **svc** *location-name* [**sequence** *sequence-number*]]

no webvpn install [**csd** *location-name* | **svc** *location-name* [**sequence** *sequence-number*]]

Syntax Description

csd *location-name*	(Optional) Installs the CSD client software package. The filename and path are entered.
svc *location-name*	(Optional) Installs the Cisco AnyConnect VPN Client software package. The filename and path are entered.
sequence *sequence-number*	(Optional) Allows for multiple packages to be installed to one gateway. If the **sequence** keyword and the *sequence-number* argument are not configured, a sequence number of 1 is applied to the package.

Command Default

Neither a CSD nor a Cisco AnyConnect VPN Client package file is installed to a WebVPN gateway.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(20)T	The **sequence** *sequence-number* keyword and argument were added.

Usage Guidelines

The installation packages must first be copied to a local file system, such as disk, flash or USB flash. The CSD and Cisco AnyConnect VPN Client software packages are pushed to end users as access is needed. The end user must have administrative privileges, and the Java Runtime Environment (JRE) for Windows version 1.4 or a later version must be installed before a CSD or Cisco AnyConnect VPN Client package can be installed.

Note Secure Sockets Layer Virtual Private Network (SSL VPN) Client (SVC) is the predecessor of Cisco AnyConnect VPN Client software.

If you have not entered the **sequence** keyword and the *sequence-number* argument and you want to install another package, you can remove the previous package (using the **no** form of the command) or you can provide another sequence number.

If you try to install a package with a sequence number that is being used, you will get an error message.

Examples

The following example shows how to install the Cisco AnyConnect VPN Client package to an SSL VPN gateway. The package is being copied to a flash file system.

```
Router(config)# webvpn install svc flash:/webvpn/svc.pkg

SSLVPN Package SSL-VPN-Client : installed successfully
```

The following example shows how to install the CSD package to an SSL VPN gateway. The package is being copied to a flash file system.

```
Router(config)# webvpn install csd flash:/securedesktop_3_1_0_9.pkg

SSLVPN Package Cisco-Secure-Desktop : installed successfully
```

The following example shows how to install Cisco AnyConnect VPN Client package to an SSL VPN gateway. The file is being copied to a USB file system.

```
Router(config)# webvpn install csd usbflash0:securedesktop-ios-3.1.1.45-k9.pkg

SSLVPN Package Cisco-Secure-Desktop : installed successfully
```

Related Commands

Command	Description
show webvpn install status	Displays the installation status of SVC or CSD client software packages.

webvpn sslvpn-vif nat

To enable Network Address Translation (NAT) on the WebVPN virtual interface, use the **webvpn sslvpn-vif nat** command in global configuration mode. To disable NAT on the WebVPN virtual interface, use the **no** form of this command.

webvpn sslvpn-vif nat {**enable** | **inside** | **outside**}

no webvpn sslvpn-vif nat {**enable** | **inside** | **outside**}

Syntax Description

enable	Enables address translation.
inside	Enables the inside interface for address translation.
outside	Enables the outside interface for address translation.

Command Default

NAT is disabled by default on the WebVPN virtual interface.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Use the **show running-config** command to verify if NAT has been enabled.

Examples

The following example shows that NAT has been enabled on the WebVPN virtual interface:

```
Router(config)# webvpn sslvpn-vif nat enable
```

Related Commands

Command	Description
show running-config	Displays the contents of the current running configuration file.

wins

To specify the primary and secondary Windows Internet Naming Service (WINS) servers, use the **wins** command in ISAKMP group configuration mode or IKEv2 authorization policy configuration mode. To remove this command from your configuration, use the **no** form of this command.

wins *primary-server* [*secondary-server*]

no wins *primary-server* [*secondary-server*]

Syntax Description

primary-server	Name of the primary WINS server.
secondary-server	(Optional) Name of the secondary WINS server.

Defaults

No primary or secondary WINS server is specified.

Command Modes

ISAKMP group configuration (config-isakmp-group)
IKEv2 authorization policy configuration (config-ikev2-author-policy)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to specify the primary and secondary WINS server for the remote access client. You must enable the following commands before enabling the **wins** command:

- **crypto isakmp client configuration group**—Specifies the group policy information that has to be defined or changed.
- **crypto ikev2 authorization policy**—Specifies the local group policy authorization parameters.

Examples

The following example shows how to define a primary and secondary WINS server for the group “cisco”:

```
crypto isakmp client configuration group cisco
  key cisco
  dns 10.2.2.2 10.3.2.3
  pool dog
  acl 199
  wins 10.1.1.2 10.1.1.3
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto ikev2 authorization policy	Specifies an IKEv2 client configuration group.
crypto isakmp client configuration group	Specifies the DNS domain to which a group belongs.

wlccp authentication-server client

To configure the list of servers to be used for 802.1X authentication, use the **wlccp authentication-server client** command in global configuration mode. To disable the server list, use the **no** form of this command.

wlccp authentication-server client {**any** | **eap** | **leap** | **mac**} *list*

no wlccp authentication-server client {**any** | **eap** | **leap** | **mac**} *list*

Syntax Description

any	Specifies client devices that use any authentication.
eap	Specifies client devices that use Extensible Authentication Protocol (EAP) authentication.
leap	Specifies client devices that use Light Extensible Authentication Protocol (LEAP) authentication.
mac	Specifies client devices that use MAC-based authentication.
list	List of client devices.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

You can specify a list of client devices that use any type of authentication, or you can specify a list of client devices that use a certain type of authentication (such as EAP, LEAP, or MAC-based authentication).

Examples

The following example shows how to configure the server list for LEAP authentication for client devices:

```
Router (config)# wlccp authentication-server client leap leap-list1
```

Related Commands

Command	Description
debug wlccp packet	Displays packet traffic to and from the WDS router.
debug wlccp wds	Displays either WDS debug state or WDS statistics messages.

Command	Description
show wlccp wds	Shows information about access points and client devices on the WDS router.
wlccp authentication-server infrastructure	Configures the list of servers to be used for 802.1X authentication for the wireless infrastructure devices.
wlccp wds priority interface	Enables a wireless device such as an access point or a wireless-aware router to be a WDS candidate.

wlccp authentication-server infrastructure

To configure the list of servers to be used for 802.1X authentication for the wireless infrastructure devices, use the **wlccp authentication-server infrastructure** command in global configuration mode. To disable the server list, use the **no** form of this command.

wlccp authentication-server infrastructure *list*

no wlccp authentication-server infrastructure *list*

Syntax Description

list	List of servers to be used for 802.1X authentication for the wireless infrastructure devices, such as access points, repeaters, and wireless-aware routers.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on Cisco Aironet access points.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Examples

This example shows how to configure the server list for 802.1X authentication for infrastructure devices participating in Cisco Centralized Key Management:

```
Router (config)# wlccp authentication-server infrastructure wlan-list1
```

Related Commands

Command	Description
debug wlccp packet	Displays packet traffic to and from the WDS router.
debug wlccp wds	Displays either WDS debug state or WDS statistics messages.
show wlccp wds	Shows information about access points and client devices on the WDS router.
wlccp authentication-server client	Configures the list of servers to be used for 802.1X authentication.
wlccp wds priority interface	Enables a wireless device such as an access point or a wireless-aware router to be a WDS candidate.

wlccp wds priority interface

To configure the router or access point to provide WDS, use the **wlccp wds priority interface** command in global configuration mode. To remove the WDS configuration from the router or access point, use the **no** form of the command .

wlccp wds priority *priority* **interface** *interface*

no wlccp wds priority *priority* **interface** *interface*

Syntax Description

priority	Priority of this WDS candidate. The valid range is from 1 to 255. The greater the priority value, the higher the priority.
interface	Interface on which the router sends out WDS advertisements. Supported interface types are as follows: • For access points—bvi • For wireless-aware routers—bvi, svi, Fast Ethernet, and Gigabit Ethernet.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced with support for Cisco Aironet access points.
12.3(11T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

The WDS candidate with the highest priority becomes the active WDS device.

Examples

This example shows how to configure the priority for an access point as a candidate to provide WDS with priority 200:

```
Router (config)# wlccp wds priority 200 interface bvi 1
```

Related Commands

Command	Description
debug wlccp packet	Displays packet traffic to and from the WDS router.
debug wlccp wds	Displays either WDS debug state or WDS statistics messages.
show wlccp wds	Shows information about access points and client devices on the WDS router.

Command	Description
wlccp authentication-server client	Configures the list of servers to be used for 802.1X authentication.
wlccp authentication-server infrastructure	Configures the list of servers to be used for 802.1X authentication for the wireless infrastructure devices.

xauth userid mode

To specify how the Easy VPN client handles extended authentication (Xauth) requests, use the **xauth userid mode** command in Cisco IOS Easy VPN remote configuration mode. To remove the setting, use the **no** form of this command.

xauth userid mode {**http-intercept | interactive | local**}

no xauth userid mode {**http-intercept | interactive | local**}

Syntax Description

http-intercept	HTTP connections are intercepted from the user through the inside interface and the prompt.
interactive	To authenticate, the user must use the command-line interface (CLI) prompts on the console. Interactive is the default behavior.
local	The saved username or password is used in the configuration.

Defaults

If the command is not configured, the default behavior is interactive.

Command Modes

Cisco IOS Easy VPN remote configuration (config-crypto-ezvpn)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

If you want to be prompted by the console, use the **interactive** keyword.

If you want to use a saved username or password, use the **local** keyword. If a local username or password is defined, the mode changes to that username or password.

Examples

The following example shows that HTTP connections will be intercepted from the user and that the user can authenticate using web-based activation:

```
crypto ipsec client ezvpn tunnel22
  connect manual
  group tunnel22 key 22tunnel
  mode client
  peer 192.168.0.1
  xauth userid mode http-intercept
!
!
interface Ethernet0
  ip address 10.4.23.15 255.0.0.0
```

```
  crypto ipsec client ezvpn tunnel22 inside !
interface Ethernet1
  ip address 192.168.0.13 255.255.255.128
  duplex auto
  crypto ipsec client ezvpn catch22
!
```

Related Commands

Command	Description
crypto ipsec client ezvpn	Creates a Cisco Easy VPN remote configuration.
debug crypto ipsec client ezvpn	Displays information about voice control messages that have been captured by the Voice DSP Control Message Logger.
debug ip auth-proxy ezvpn	Displays information related to proxy authentication behavior for web-based activation.
show crypto ipsec client ezvpn	Displays the Cisco Easy VPN Remote configuration.
show ip auth-proxy	Displays the authentication proxy entries or the running authentication proxy configuration.

zone-member security

To attach an interface to a security zone, use the **zone-member security** command in interface configuration mode. To detach the interface from a zone, use the **no** form of this command.

zone-member security *zone_name*

no zone-member security *zone_name*

Syntax Description

zone_name	Name of the security zone to which an interface is attached.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The **zone-member security** command puts an interface into a security zone. When an interface is in a security zone, all traffic to and from that interface (except traffic going to the router or initiated by the router) is dropped by default. To permit traffic through an interface that is a zone member, you must make that zone part of a zone-pair to which you apply a policy. If the policy permits traffic (via **inspect** or **pass** actions), traffic can flow through the interface.

Examples

The following example attaches interface e0 to the zone z1:

```
interface e0
 zone-member security z1
```

Related Commands

Command	Description
zone security	Creates a zone.

zone pair security

To create a zone pair, use the **zone-pair security** command in global configuration mode. To delete a zone pair, use the **no** form of this command.

zone-pair security *zone-pair-name* **source** {*source-zone-name* | **self** | **default**} **destination** {*destination-zone-name* | **self** | **default**}

no zone-pair security *zone-pair-name* **source** {*source-zone-name* | **self** | **default**} **destination** {*destination-zone-name* | **self** | **default**}

Syntax Description

zone-pair-name	Name of the zone being attached to an interface.
source *source-zone-name*	Specifies the name of the router from which traffic is originating.
default	Specifies the name of the default security zone. Interfaces without configured zones belong to the default zone.
destination *destination-zone-name*	Specifies the name of the router to which traffic is bound.
self	Specifies the system-defined zone. Indicates whether traffic will be going to or from a router.

Command Default

A zone pair is not created.

Command Modes

Global configuration (config)

CommandHistory

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.6	This command was modified. The **default** keyword was added.

Usage Guidelines

This command creates a zone-pair, which permits a unidirectional firewall policy between a pair of security zones. After you enter this command, you can enter the **service-policy type inspect** command.

If you created only one zone, you can use the system-defined default zone (self) as part of a zone-pair. Such a zone pair and its associated policy applies to traffic directed to the router or generated by the router. It does not affect traffic through the router.

You can specify the **self** keyword for the source or destination, but not for both. You cannot modify or unconfigure the self zone. You can specify the **default** keyword to include all the interfaces that are not configured with any other zones. However, the default zone needs to be defined before it can be used in a zone pair.

Examples

The following example shows how to create zones z1 and z2, identify them, and create a zone pair where z1 is the source and z2 is the destination:

```
zone security z1
 description finance department networks

zone security z2
 description engineering services network

zone-pair security zp source z1 destination z2

zone-pair security
```

The following example shows how to define zone pair z1-z2 and attach the service policy p1 to the zone pair:

```
zone-pair security zp source z1 destination z2
 service-policy type inspect p1
```

The following example shows how the zone pair is configured between system-defined and default zones.

```
zone security default

class-map type inspect match-all tcp-traffic
   match protocol tcp
   match access-group 199

policy-map type inspect p1
   class type inspect tcp-traffic

zone-pair security self-default-zp source self destination default
   service-policy type inspect p1
```

Related Commands

Command	Description
zone-member security	Attaches an interface to a security zone.
zone-pair	Creates a zone pair.

zone security

To create a security zone, use the **zone security** command in global configuration mode. To delete a security zone, use the **no** form of this command.

zone security {*zone-name* | **default**}

no zone security {*zone-name* | **default**}

Syntax Description

zone-name	Name of the security zone. You can enter up to 256 alphanumeric characters.
default	Specifies the name of a default security zone. Interfaces that are not configured on any of the security zones belong to the default zone.

Command Default

There is a system-defined “self” zone.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.6	This command was modified. The **default** keyword was added.

Usage Guidelines

We recommend that you create at least two security zones so that you can create a zone pair. If you create only one zone, you can use the default system-defined self zone. The self zone cannot be used for traffic going through a router. You can specify the **default** keyword to include all the interfaces that are not configured with any other zones.

To configure an interface to be a member of a security zone, use the **zone-member security** command.

Examples

The following example shows how to create and describe zones x1 and z1:

```
zone security x1
 description testzonex

zone security z1
 description testzonez
```

The following example shows how to create a default zone:

```
zone security default
 description system level default zone
```

Related Commands

Command	Description
description (identify zone)	Contains a description of a zone.
zone-member security	Attaches an interface to a zone.
zone-pair security	Creates a zonepair.